De Hill-cipher herzien

Bachelorscriptie

Tim Verheijen

8 september 2009

Begeleider: Dr. W. Bosma

Tweede lezer: Prof. dr. M. Gehrke

Radboud Universiteit Nijmegen

Inhoudsopgave

Samenvatting

De Hill-cipher is een cryptosysteem dat bedacht is door Lester Hill in 1929. Het doel van een cryptosysteem is om boodschappen te coderen (en decoderen), opdat het bericht niet door personen met kwade bedoelingen kan worden gelezen. Aan dit door Lester Hill bedachte systeem zaten echter enkele haken en ogen. De Hill-cipher was namelijk eenvoudig te kraken met behulp van een zogenaamde plaintext attack.

In deze bachelorscriptie doen we een suggestie voor een aangepaste Hill-cipher, in de hoop deze veiliger te maken. Er blijkt echter dat er ook voor de vernieuwde Hill-cipher een tweetal methoden te vinden is om de (de)codeersleutel(s) te achterhalen. Eerst zullen deze methoden worden uiteengezet voor sleutellengte 2. Vervolgens worden de twee methoden gegeneraliseerd naar een willekeurige sleutellengte.

Voorwoord

Zolang als we bestaan hebben we al geheimen voor anderen. Vaak gaat het om iets kleins en onschuldigs, maar er zijn situaties waarin het toch zeer wenselijk is dat niemand de informatie kan onderscheppen. De technieken die het mogelijk maken om informatie te beschermen behoren tot het veld van de cryptografie. In het algemeen verstaat men onder cryptografie "het proces van het ontwerpen van cryptosystemen".

In de komende hoofdstukken zullen we uitgaan we twee personen, genaamd Alice en Bob, die met elkaar willen communiceren. Alice wil een boodschap, de *plaintext*, naar Bob versturen en met behulp van een *encryptiesleutel* codeert zij deze plaintext volgens een methode die zij van tevoren samen met Bob heeft afgesproken. Bob ontvangt de gecodeerde boodschap, die we de *ciphertext* noemen. Tot slot decodeert Bob de ciphertext met een *decryptiesleutel*, zodat hij de oorspronkelijke boodschap kan lezen. (Meestal worden de termen encryptiesleutel en decryptiesleutel allebei verkort tot "sleutel", omdat vaak uit de context al blijkt welke sleutel er bedoeld wordt.)

Tijdens het hele gebeuren is er echter een afluisteraar die luistert naar de naam Eve. Verondersteld wordt dat Eve weet welk cryptosysteem Alice en Bob gebruiken en dat zij de geëncrypte plaintext weet te onderscheppen, maar de sleutel kent zij niet. Eve wil uiteraard graag weten wat Alice en Bob te bespreken hebben en daarom probeert zij de sleutel te achterhalen, zodat zij in het vervolg elke onderschepte ciphertext kan decoderen.

Een plaintext zullen we in het vervolg aangeven met kleine letters: `plaintext`. Een ciphertext noteren we met grote letters: `CIPHERTEXT`.

Omdat veel cryptosystemen gebaseerd zijn op getallen en berekeningen, schrijven we een plaintext vaak eerst als een rijtje van getallen of als rijvector. Hierbij geldt $a = 0$, $b = 1$, $c = 2$, ..., $z = 25$. De plaintext `hoi` kunnen we dus ook noteren als (7 14 8). Stel dat (7 14 8) gecodeerd wordt naar (3 0 6), dan kunnen we op soortgelijke wijze zien dat de ciphertext `DAG` is. Omdat het alfabet 26 letters telt, is het gebruikelijk om modulo 26 te rekenen. In het eerste hoofdstuk zullen we zien dat het verschuiven van letters in de plaintext een manier van coderen is. Als we dan bijvoorbeeld de plaintextletter `v`, oftewel het getal 21, veertien letters naar rechts willen verschuiven, dan krijgen we als ciphertext het getal 35. En omdat we hadden gezegd dat $a = 0$, $b = 1$, $c = 2$, ..., $z = 25$, volgt dat we het getal 35 aan geen enkele letter hebben toegekend. Vandaar dat het rekenen modulo 26 ons uitkomst biedt; dan krijgen we immers altijd een welgedefineerde ciphertext(letter). (We zien dat $35 \equiv 9 \pmod{26}$ en we krijgen `v` $\mapsto$ `J`.)

Tim Verheijen
studentnummer 0513350
timverheijen@student.ru.nl

1 Inleiding

1.1 Klassieke cryptosystemen

Onder de 'klassieke' cryptosystemen verstaan we de cryptosystemen waarbij Alice en Bob eerst afspreken welke sleutel ze gaan gebruiken, voordat ze daadwerkelijk boodschappen versturen. Bij veel van deze cryptosystemen is er sprake van weinig diffusie. Dit wil zeggen dat wanneer er een letter in de plaintext wordt gewijzigd, er weinig letters veranderen in de ciphertext.

Een voorbeeld van een dergelijk klassiek cryptosysteem met weinig diffusie is de Caesarverschuiving. Deze methode is vernoemd naar Julius Caesar, omdat zij in de tijd van de Romeinen ook daadwerkelijk gebruikt werd om boodschappen aan legeraanvoerders door te geven. De Caesarverschuiving is erop gebaseerd om elke letter van de plaintext met een van tevoren gekozen getal (of letter dus) te laten verschuiven. Dit getal (deze letter) is de sleutel. Bij het wijzigen van een letter in de plaintext verandert er ook maar een letter in de ciphertext.

Voorbeeld 1.1. Stel dat Caesar de letter `c` als sleutel heeft gekozen en dat hij de plaintext `vallimburgaan` wil overbrengen naar zijn legeraanvoerders. Aangezien `c` $= 2$, wordt elke letter in de plaintext twee letters in het alfabet opgeschoven. Dit betekent dat `v` $\mapsto$ `X`, `a` $\mapsto$ `C`, etc. We zien dat de plaintext `vallimburgaan` uiteindelijk gecodeerd wordt naar de ciphertext `XCNNKODWTICCP`. $\triangleleft$

Bij cryptosystemen als de Caesarverschuiving is het betrekkelijk eenvoudig om de code te kraken en de sleutel te vinden. Des te langer de plaintext namelijk is, des te waarschijnlijker het is dat veel voorkomende letters in de (oorspronkelijke) taal ook vaak in de plaintext voorkomen. De `e` is in de Nederlandse taal bijvoorbeeld de meest frequente letter. Als we een Nederlandstalig boek zouden coderen met behulp van een Caesarverschuiving, dan zouden we eenvoudig kunnen achterhalen naar welke letter de `e` is gecodeerd, namelijk de letter die in de ciphertext het vaakst voorkomt.[1] Op deze manier kunnen we de sleutel afleiden.

De kleine sleutelruimte bij de Caesarverschuiving maakt het systeem ook niet veiliger. Omdat er maar 26 letters in het alfabet zitten, zijn er slechts 26 mogelijkheden voor de sleutel. Door alle mogelijkheden na te lopen – de zogenaamde *brute force attack* – kan de sleutel vrij snel achterhaald worden. Een grote sleutelruimte is dus gewenst, opdat een brute force attack minder kans maakt om de sleutel te kraken.

Het gebruik van blokken van letters en een hierbij corresponderende sleutel van dezelfde lengte maakt het al een stuk lastiger om een succesvolle frequentieanalyse op de desbetreffende plaintext los te laten. Bij deze zogenaamde *block ciphers* worden blokken van letters in een klap gecodeerd naar een blok (van dezelfde lengte) in de ciphertext.

1.2 De Hill-cipher

Een voorbeeld van een block cipher is de Hill-cipher, bedacht door Lester Hill in 1929. Hoewel dit cryptosysteem – voor zover bekend is – niet vaak is gebruikt, speelt de Hill-cipher wel een significante rol in de geschiedenis van de cryptografie. Vermoed wordt namelijk dat de Hill-cipher

[1] We spreken hier van 'eenvoudig' in de zin dat het makkelijk is; niet in de zin dat het klusje snel geklaard is. Er zijn leukere hobby's te verzinnen dan het turven van alle letters in een boek.

het eerste cryptosysteem was dat gebruik maakte van algebraïsche methoden. Tegenwoordig zijn deze methoden niet weg te denken uit de cryptografie.

De Hill-cipher is gebaseerd op het vermenigvuldigen van een rijvector (de plaintext) met een vast gekozen matrix K (de sleutel). De uitkomst, opnieuw een rijvector, wordt modulo 26 gedaan en dit levert de ciphertext op.

Voorbeeld 1.2. We kiezen eerst een natuurlijk getal n als lengte van elk blok letters, bijvoorbeeld $n = 3$. De sleutel is een $n \times n$ matrix K, bijvoorbeeld $K = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$.
Stel we willen de boodschap `abc` verzenden. Hier maken we eerst een rijvector van: `abc` wordt (0 1 2). Vervolgens gooien we de matrix K er van de rechterkant tegenaan en reduceren de uitkomst modulo 26:

$$(0\ 1\ 2) \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \equiv (0\ 23\ 22) \qquad (\text{mod } 26)$$

En dus is de ciphertext `AXW`. ◁

Om de ciphertext te decoderen is het nodig dat ggd(det(K),26) = 1, anders zouden er meerdere boodschappen op dezelfde ciphertext kunnen worden afgebeeld en dus zou Bob de boodschap van Alice nooit met zekerheid kunnen bepalen.

Voorbeeld 1.3. De determinant van de in het vorige voorbeeld gebruikte matrix K is det(K) $= -3$ en dus geldt ggd(det(K),26) = 1. In een visioen zien we plotseling dat

$$K^{-1} = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}.$$

(Uiteraard kan de lezer dit zelf ook nog narekenen.) We kunnen de ciphertext `AXW` nu decoderen door te vermenigvuldigen met de inverse van de sleutel K:

$$(0\ 23\ 22) \cdot K^{-1} \equiv (0\ 23\ 22) \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix} \equiv (0\ 1\ 2) \quad (\text{mod } 26).$$

◁

Het is lastig om de sleutel te vinden bij de Hill-cipher wanneer alleen de ciphertext bekend is (ook wel *ciphertext only attack* genoemd).[2] Een nadeel van de Hill-cipher is dat dit cryptosysteem slecht bestand is tegen een zogenaamde *plaintext attack*. Zo'n plaintext attack houdt in dat Eve tijdelijk de beschikking krijgt over de sleutel, maar zij kent deze niet. Wel heeft zij de mogelijkheid om een plaintext naar keuze te nemen en kijken naar welke ciphertext de sleutel ons stuurt. We kunnen dit opvatten als een soort snoepautomaat waarbij Eve een booschap intoetst, maar zij kan niet zien wat er allemaal voor lekkers in de snoepautomaat zit. Nadat zij echter de boodschap heeft ingetoetst, valt er een Mars of een Twix of een ... [vul lekkernij

[2] Cryptoanalyse gebaseerd op letterfrequentie werkt niet bij een Hill-cipher, omdat er in een klap blokken van letters worden gecodeerd.

naar keuze in] uit de automaat; nu weet zij een plaintext-ciphertext combinatie. Aan de hand van een voorbeeld zullen we aantonen hoe eenvoudig het is om de Hill-cipher te kraken, dat wil zeggen de sleutel te achterhalen, met behulp van een plaintext attack.

Voorbeeld 1.4. Als eerste moet Eve bepalen welke lengte de sleutel heeft. Hier is geen slimme manier voor; zij zal enkele waarden moeten proberen totdat ze de goede sleutellengte n heeft gevonden. In deze scriptie zullen we veronderstellen dat n bekend is.
Stel dat $n = 2$. Dit betekent dat K een 2×2 matrix is en dat K dus vier getallen bevat. We kijken, in twee blokjes van twee letters per keer, welke ciphertext bij een zekere plaintext hoort. We nemen als plaintext `cryptografie`, hetgeen neerkomt op de volgende getallenparen:

$$2\ \ 17 \qquad 24\ \ 15 \qquad 19\ \ 14 \qquad 6\ \ 17 \qquad 0\ \ 5 \qquad 8\ \ 4$$

Volgens onze snoepautomaat blijkt hier de volgende ciphertext bij te horen:

$$25\ \ 22 \qquad 18\ \ 4 \qquad 13\ \ 7 \qquad 20\ \ 18 \qquad 15\ \ 11 \qquad 9\ \ 21$$

De eerste twee blokken leiden tot de volgende matrixvergelijking, waarbij K de sleutel is die zich in de snoepautomaat bevindt:

$$\begin{pmatrix} 2 & 17 \\ 24 & 15 \end{pmatrix} \cdot K \equiv \begin{pmatrix} 25 & 22 \\ 18 & 4 \end{pmatrix} \pmod{26}$$

(Merk op dat we hierboven geen rijvector maar een matrix als plaintext hebben genomen. In theorie hadden we ook eerst de rijvector (2 17) kunnen nemen en vervolgens (24 15), maar omdat de eerste rij van de ciphertextmatrix alleen afhangt van de eerste rijvector en de tweede rij van de ciphertextmatrix alleen afhankelijk is van de tweede rijvector, kunnen we twee vliegen in een klap slaan.) Helaas kunnen we K niet bepalen, omdat $\det(\begin{pmatrix} 2 & 17 \\ 24 & 15 \end{pmatrix}) = -408$ en dus is de matrix $\begin{pmatrix} 2 & 17 \\ 24 & 15 \end{pmatrix}$ niet inverteerbaar modulo 26 is. Daarom proberen we een andere combinatie:

$$\begin{pmatrix} 2 & 17 \\ 19 & 14 \end{pmatrix} \cdot K \equiv \begin{pmatrix} 25 & 22 \\ 13 & 7 \end{pmatrix} \pmod{26}$$

De matrix $\begin{pmatrix} 2 & 17 \\ 19 & 14 \end{pmatrix}$ is wél inverteerbaar en dus volgt:

$$K \equiv \begin{pmatrix} 2 & 17 \\ 19 & 14 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 17 \\ 19 & 14 \end{pmatrix} \cdot K \equiv \begin{pmatrix} 2 & 17 \\ 19 & 14 \end{pmatrix}^{-1} \begin{pmatrix} 25 & 22 \\ 13 & 7 \end{pmatrix} \equiv \begin{pmatrix} 10 & 25 \\ 5 & 20 \end{pmatrix} \pmod{26}$$

En dus hebben we met zeer weinig inspanning de sleutel K gevonden. ◁

Samenvatting 1.5. In dit hoofdstuk hebben we de Hill-cipher geïntroduceerd. Lang zijn we er niet van onder de indruk geweest, want de Hill-cipher is eenvoudig te kraken met behulp van een plaintext attack. Hier volgt een samenvatting van hoe dit in z'n werk gaat:

- Probeer enkele sleutellengtes n, totdat de juiste sleutellengte gevonden is. (Dit is meteen de lastigste stap van allemaal; hier is verder geen handige methode voor.)
- Kies een plaintext P zodanig dat P inverteerbaar is modulo 26 en bepaal wat de hierbij horende ciphertext C is.
- Bereken de sleutel $K \equiv P^{-1} \cdot C \pmod{26}$.

◁

2 Sleutellengte $n = 2$

2.1 Twee sleutels

In het vorige hoofdstuk hebben we gezien dat de Hill-cipher makkelijk te kraken is met behulp van een plaintext attack. De vraag is nu of we de Hill-cipher dusdanig kunnen aanpassen dat het achterhalen van de sleutel minder eenvoudig wordt. Een idee om de boodschap beter te coderen is om niet een, maar twee sleutels te gebruiken. We zouden de tot rijvector gemaakte plaintext met een matrix K_1 kunnen vermenigvuldigen, zoals we in hoofdstuk 1 gedaan hebben, en vervolgens de ontstane rijvector nogmaals vermenigvuldigen met een matrix K_2. Dit levert echter geen nieuwe of spannende situaties op, want wat we hier doen komt op hetzelfde neer als de Hill-cipher met matrix $K := K_1 \cdot K_2$.

Het is dus niet de moeite waard om de rijvector tweemaal van rechts met een sleutel te vermenigvuldigen. Maar wat zou er gebeuren als we van links met een matrix K_l vermenigvuldigen en rechts met een matrix K_r? Merk op dat het vermenigvuldigen van een matrix met een rijvector (in die volgorde) niet goed gaat. We zouden van de rijvector een kolomvector kunnen maken en de na de eerste vermenigvuldiging ontstane kolomvector kantelen tot een rijvector voor de tweede matrixvermenigvuldiging, maar we kiezen ervoor om de plaintext zelf ook als matrix te schrijven, zodat we drie $n \times n$ matrices krijgen. De ciphertext komt dus ook als een $n \times n$ matrix uit onze geüpdatete snoepautomaat rollen. (Dit hadden we bij de oorspronkelijke Hill-cipher ook kunnen doen: het nemen van een matrix (in plaats van een rijvector) als plaintext en vervolgens vermenigvuldigen met een (sleutel)matrix K.)

Er zijn nu twee prangende vragen waar we graag een antwoord op zouden willen krijgen:

- Is het vermenigvuldigen van links met een matrix K_l en het vermenigvuldigen van rechts met een matrix K_r wezenlijk anders dan de (aangepaste) Hill-cipher (i.e. het enkel vermenigvuldigen van rechts met een matrix K) of komt dit op hetzelfde neer?
- (*Indien de nieuwe Hill-cipher inderdaad anders is dan de originele Hill-cipher.*) Zijn de sleutels K_l en K_r bij het links respectievelijk rechts vermenigvuldigen van de plaintext makkelijk te achterhalen, zoals ook de sleutel bij de Hill-cipher makkelijk te achterhalen is?

Opmerking 2.1. In dit hoofdstuk zullen we niet modulo 26 rekenen, maar modulo 29. De reden hiervoor is dat $\mathbb{F}_{29}$ een lichaam is, daar waar $\mathbb{F}_{26}$ dat niet is. We willen namelijk gebruikmaken van de mooie eigenschap dat elk element in $\mathbb{F}_{29}$ een inverse heeft. We moeten nu nog een letter aan de getallen 26, 27, 28 toekennen, maar het hele alfabet kent zijn plekje al. Vandaar dat we afspreken dat $a = 0$, $b = 1$, $c = 2$, ..., $z = 25$, [spatie]=26, [komma]=27 en [punt]=28. Vanaf nu zouden we dus ook de boodschap `hiep hoi.` kunnen verzenden. ◁

2.2 Apocalyps

Voordat we dieper op deze kernvragen ingaan, zijn we natuurlijk eerst benieuwd wat voor nut het heeft als we, of liever gezegd, als Eve de sleutels K_l en K_r kent.

Laat P de plaintext, K_l de linkersleutel, K_r de rechtersleutel en C de ciphertext zijn. Hierbij zijn K_l en K_r inverteerbaar, zodat elke ciphertext slechts één plaintext kan hebben (wel zo

makkelijk voor Bob bij het decoderen). Als geldt $K_l \cdot P \cdot K_r \equiv C \pmod{29}$ en Eve kent K_l en K_r, dan voelen we de hete kolen onder onze voeten wanneer Eve een ciphertext C onderschept. Immers: $\det(K_l) \neq 0$ en $\det(K_r) \neq 0$ en dus bestaan K_l^{-1}, K_r^{-1}. Eve kan nu $P \equiv K_l^{-1} \cdot C \cdot K_r^{-1} \pmod{29}$ uitrekenen voor elke C. En dit is dus niet bepaald waar we op uit zijn.

2.3 Verschillend of toch hetzelfde?

Vanaf nu zullen we ons specifiek richten op Hill-ciphers met sleutels ter lengte $n = 2$. Naderhand zal blijken dat we onderstaande theorieën en methodes ook kunnen generaliseren naar een willekeurige sleutellengte $n \in \mathbb{N}^*$.

Zij $P = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix}$, $K_l = \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix}$, $K_r = \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix}$ en $C = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$, waar P opnieuw de plaintext is (p_1 is de eerste letter van het blok, p_2 de tweede, etc.), K_l is de linkersleutel, K_r is de rechtersleutel en C is de ciphertext (voor alle $i \in \{1, 2, 3, 4\}$ is c_i ook hier weer de i^{de} letter van de ciphertext). Dan geldt achtereenvolgens (mod 29):

$$
\begin{aligned}
K_l \cdot P \cdot K_r &\equiv \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \\
&\equiv \begin{pmatrix} l_1p_1 + l_2p_3 & l_1p_2 + l_2p_4 \\ l_3p_1 + l_4p_3 & l_3p_2 + l_4p_4 \end{pmatrix} \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \\
&\equiv \begin{pmatrix} (l_1p_1 + l_2p_3)r_1 + (l_1p_2 + l_2p_4)r_3 & (l_1p_1 + l_2p_3)r_2 + (l_1p_2 + l_2p_4)r_4 \\ (l_3p_1 + l_4p_3)r_1 + (l_3p_2 + l_4p_4)r_3 & (l_3p_1 + l_4p_3)r_2 + (l_3p_2 + l_4p_4)r_4 \end{pmatrix} \\
&\equiv \begin{pmatrix} l_1p_1r_1 + l_2p_3r_1 + l_1p_2r_3 + l_2p_4r_3 & l_1p_1r_2 + l_2p_3r_2 + l_1p_2r_4 + l_2p_4r_4 \\ l_3p_1r_1 + l_4p_3r_1 + l_3p_2r_3 + l_4p_4r_3 & l_3p_1r_2 + l_4p_3r_2 + l_3p_2r_4 + l_4p_4r_4 \end{pmatrix} \\
&\equiv \begin{pmatrix} p_1(l_1r_1) + p_2(l_1r_3) + p_3(l_2r_1) + p_4(l_2r_3) & p_1(l_1r_2) + p_2(l_1r_4) + p_3(l_2r_2) + p_4(l_2r_4) \\ p_1(l_3r_1) + p_2(l_3r_3) + p_3(l_4r_1) + p_4(l_4r_3) & p_1(l_3r_2) + p_2(l_3r_4) + p_3(l_4r_2) + p_4(l_4r_4) \end{pmatrix} \\
&\equiv \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}
\end{aligned}
$$

Stel nu dat $K_l \cdot P \cdot K_r \equiv P \cdot M \pmod{29}$, voor een zekere matrix $M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$ met $m_1, m_2, m_3, m_4 \in \mathbb{Z}$. Met andere woorden: stel dat onze nieuwe Hill-cipher op hetzelfde neerkomt als een oorspronkelijke Hill-cipher met sleutel M. Dan moet gelden (mod 29):

$$
\begin{aligned}
K_l \cdot P \cdot K_r &\equiv P \cdot M \\
&\equiv \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \\
&\equiv \begin{pmatrix} p_1m_1 + p_2m_3 & p_1m_2 + p_2m_4 \\ p_3m_1 + p_4m_3 & p_3m_2 + p_4m_4 \end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
\implies \quad p_1(l_1r_1) + p_2(l_1r_3) + p_3(l_2r_1) + p_4(l_2r_3) &\equiv p_1m_1 + p_2m_3 \quad (1) \\
p_1(l_1r_2) + p_2(l_1r_4) + p_3(l_2r_2) + p_4(l_2r_4) &\equiv p_1m_2 + p_2m_4 \quad (2) \\
p_1(l_3r_1) + p_2(l_3r_3) + p_3(l_4r_1) + p_4(l_4r_3) &\equiv p_3m_1 + p_4m_3 \quad (3) \\
p_1(l_3r_2) + p_2(l_3r_4) + p_3(l_4r_2) + p_4(l_4r_4) &\equiv p_3m_2 + p_4m_4 \quad (4)
\end{aligned}
$$

Uit (1) volgt nu (mod 29):

$$m_1 \equiv l_1r_1 + \frac{p_2}{p_1}(l_1r_3 - m_3) + \frac{p_3}{p_1}(l_2r_1) + \frac{p_4}{p_1}(l_2r_3) \tag{5}$$

$$\begin{aligned}
\Longrightarrow \quad p_1(l_3r_1) + p_2(l_3r_3) + p_3(l_4r_1) + p_4(l_4r_3) &\overset{(3)}{\equiv} p_3m_1 + p_4m_3 \\
&\overset{(5)}{\equiv} p_3(l_1r_1) + \frac{p_2p_3}{p_1}(l_1r_3 - m_3) + \frac{p_3^2}{p_1}(l_2r_1) \\
&\quad + \frac{p_3p_4}{p_1}(l_2r_3) + p_4m_3 \\
&\equiv p_3(l_1r_1) + \frac{p_2p_3}{p_1}(l_1r_3) + \frac{p_3^2}{p_1}(l_2r_1) \\
&\quad + \frac{p_3p_4}{p_1}(l_2r_3) + (p_4 - \frac{p_2p_3}{p_1})m_3
\end{aligned}$$

$$\begin{aligned}
\Longrightarrow \quad m_3(p_4 - \frac{p_2p_3}{p_1}) &\equiv p_1(l_3r_1) + p_2(l_3r_3) + p_3(l_4r_1) + p_4(l_4r_3) \\
&\quad -p_3(l_1r_1) - \frac{p_2p_3}{p_1}(l_1r_3) - \frac{p_3^2}{p_1}(l_2r_1) - \frac{p_3p_4}{p_1}(l_2r_3)
\end{aligned}$$

$$\begin{aligned}
\Longrightarrow \quad m_3(p_1p_4 - p_2p_3) &\equiv p_1^2(l_3r_1) + p_1p_2(l_3r_3) + p_1p_3(l_4r_1) + p_1p_4(l_4r_3) \\
&\quad -p_1p_3(l_1r_1) - p_2p_3(l_1r_3) - p_3^2(l_2r_1) - p_3p_4(l_2r_3)
\end{aligned}$$

$$\begin{aligned}
\Longrightarrow \quad m_3 &\equiv \frac{1}{p_1p_4 - p_2p_3} \cdot \Big(p_1^2(l_3r_1) + p_1p_2(l_3r_3) + p_1p_3(l_4r_1) + p_1p_4(l_4r_3) \qquad (6) \\
&\quad -p_1p_3(l_1r_1) - p_2p_3(l_1r_3) - p_3^2(l_2r_1) - p_3p_4(l_2r_3)\Big) \\
&\equiv \frac{p_1^2}{p_1p_4 - p_2p_3}(l_3r_1) + \frac{p_1p_2}{p_1p_4 - p_2p_3}(l_3r_3) + \frac{p_1p_3}{p_1p_4 - p_2p_3}(l_4r_1) \qquad (7) \\
&\quad + \frac{p_1p_4}{p_1p_4 - p_2p_3}(l_4r_3) - \frac{p_1p_3}{p_1p_4 - p_2p_3}(l_1r_1) - \frac{p_2p_3}{p_1p_4 - p_2p_3}(l_1r_3) \\
&\quad - \frac{p_3^2}{p_1p_4 - p_2p_3}(l_2r_1) - \frac{p_3p_4}{p_1p_4 - p_2p_3}(l_2r_3)
\end{aligned}$$

$\Longrightarrow$

$$\begin{aligned}
m_1 &\overset{(5)}{\equiv} l_1r_1 + \frac{p_2}{p_1}(l_1r_3 - m_3) + \frac{p_3}{p_1}(l_2r_1) + \frac{p_4}{p_1}(l_2r_3) \\
&\overset{(6)}{\equiv} l_1r_1 + \frac{p_2}{p_1}(l_1r_3) + \frac{p_3}{p_1}(l_2r_1) + \frac{p_4}{p_1}(l_2r_3) - \frac{p_2}{p_1} \cdot \frac{1}{p_1p_4 - p_2p_3} \cdot \Big(p_1^2(l_3r_1) + p_1p_2(l_3r_3) \\
&\quad + p_1p_3(l_4r_1) + p_1p_4(l_4r_3) - p_1p_3(l_1r_1) - p_2p_3(l_1r_3) - p_3^2(l_2r_1) - p_3p_4(l_2r_3)\Big) \\
&\equiv l_1r_1 + \frac{p_2}{p_1}(l_1r_3) + \frac{p_3}{p_1}(l_2r_1) + \frac{p_4}{p_1}(l_2r_3) + \frac{1}{p_1p_4 - p_2p_3} \cdot \Big(- p_1p_2(l_3r_1) - p_2^2(l_3r_3) \\
&\quad - p_2p_3(l_4r_1) - p_2p_4(l_4r_3) + p_2p_3(l_1r_1) + \frac{p_2^2p_3}{p_1}(l_1r_3) + \frac{p_2p_3^2}{p_1}(l_2r_1) + \frac{p_2p_3p_4}{p_1}(l_2r_3)\Big)
\end{aligned}$$

$$
\begin{aligned}
\equiv\ & (1+\frac{p_2p_3}{p_1p_4-p_2p_3})(l_1r_1)+\frac{p_2}{p_1}(1+\frac{p_2p_3}{p_1p_4-p_2p_3})(l_1r_3)+\frac{p_3}{p_1}(1+\frac{p_2p_3}{p_1p_4-p_2p_3})(l_2r_1)\\
& +\frac{p_4}{p_1}(1+\frac{p_2p_3}{p_1p_4-p_2p_3})(l_2r_3)-\frac{p_1p_2}{p_1p_4-p_2p_3}(l_3r_1)-\frac{p_2^2}{p_1p_4-p_2p_3}l_3r_3-\frac{p_2p_3}{p_1p_4-p_2p_3}(l_4r_1)\\
& -\frac{p_2p_4}{p_1p_4-p_2p_3}(l_4r_3)\\
\equiv\ & \frac{p_1p_4}{p_1p_4-p_2p_3}(l_1r_1)+\frac{p_2}{p_1}\frac{p_1p_4}{p_1p_4-p_2p_3}(l_1r_3)+\frac{p_3}{p_1}\frac{p_1p_4}{p_1p_4-p_2p_3}(l_2r_1)+\frac{p_4}{p_1}\frac{p_1p_4}{p_1p_4-p_2p_3}(l_2r_3)\\
& -\frac{p_1p_2}{p_1p_4-p_2p_3}(l_3r_1)-\frac{p_2^2}{p_1p_4-p_2p_3}l_3r_3-\frac{p_2p_3}{p_1p_4-p_2p_3}(l_4r_1)-\frac{p_2p_4}{p_1p_4-p_2p_3}(l_4r_3)\\
\equiv\ & \frac{p_1p_4}{p_1p_4-p_2p_3}(l_1r_1)+\frac{p_2p_4}{p_1p_4-p_2p_3}(l_1r_3)+\frac{p_3p_4}{p_1p_4-p_2p_3}(l_2r_1)+\frac{p_4^2}{p_1p_4-p_2p_3}(l_2r_3)\\
& -\frac{p_1p_2}{p_1p_4-p_2p_3}(l_3r_1)-\frac{p_2^2}{p_1p_4-p_2p_3}(l_3r_3)-\frac{p_2p_3}{p_1p_4-p_2p_3}(l_4r_1)-\frac{p_2p_4}{p_1p_4-p_2p_3}(l_4r_3)
\end{aligned}
$$

We hebben nu m_1 en m_3 uitgedrukt in termen van p_i, l_i en r_i met $i \in \{1,2,3,4\}$. Ditzelfde kunnen we uiteraard doen voor m_2 en m_4. Uit (2) volgt namelijk (mod 29):

$$
m_2 \equiv l_1r_2+\frac{p_2}{p_1}(l_1r_4-m_4)+\frac{p_3}{p_1}(l_2r_2)+\frac{p_4}{p_1}(l_2r_4) \tag{8}
$$

$$
\begin{aligned}
\Longrightarrow \quad p_1(l_3r_2)+p_2(l_3r_4)+p_3(l_4r_2)+p_4(l_4r_4) &\overset{(4)}{\equiv} p_3m_2+p_4m_4\\
&\overset{(8)}{\equiv} p_3(l_1r_2)+\frac{p_2p_3}{p_1}(l_1r_4-m_4)+\frac{p_3^2}{p_1}(l_2r_2)\\
&\quad +\frac{p_3p_4}{p_1}(l_2r_4)+p_4m_4\\
&\equiv p_3(l_1r_2)+\frac{p_2p_3}{p_1}(l_1r_4)+\frac{p_3^2}{p_1}(l_2r_2)\\
&\quad +\frac{p_3p_4}{p_1}(l_2r_4)+(p_4-\frac{p_2p_3}{p_1})m_4
\end{aligned}
$$

$$
\begin{aligned}
\Longrightarrow \quad m_4(p_4-\frac{p_2p_3}{p_1}) &\equiv p_1(l_3r_2)+p_2(l_3r_4)+p_3(l_4r_2)+p_4(l_4r_4)\\
&\quad -p_3(l_1r_2)-\frac{p_2p_3}{p_1}(l_1r_4)-\frac{p_3^2}{p_1}(l_2r_2)-\frac{p_3p_4}{p_1}(l_2r_4)
\end{aligned}
$$

$$
\begin{aligned}
\Longrightarrow \quad m_4(p_1p_4-p_2p_3) &\equiv p_1^2(l_3r_2)+p_1p_2(l_3r_4)+p_1p_3(l_4r_2)+p_1p_4(l_4r_4)\\
&\quad p_1p_3(l_1r_2)-p_2p_3(l_1r_4)-p_3^2(l_2r_2)-p_3p_4(l_2r_4)
\end{aligned}
$$

$$
\begin{aligned}
\Longrightarrow \quad m_4 &\equiv \frac{1}{p_1p_4-p_2p_3}\cdot\Big(p_1^2(l_3r_2)+p_1p_2(l_3r_4)+p_1p_3(l_4r_2)+p_1p_4(l_4r_4) \qquad (9)\\
&\quad -p_1p_3(l_1r_2)-p_2p_3(l_1r_4)-p_3^2(l_2r_2)-p_3p_4(l_2r_4)\Big)\\
&\equiv \frac{p_1^2}{p_1p_4-p_2p_3}(l_3r_2)+\frac{p_1p_2}{p_1p_4-p_2p_3}(l_3r_4)+\frac{p_1p_3}{p_1p_4-p_2p_3}(l_4r_2) \qquad (10)\\
&\quad +\frac{p_1p_4}{p_1p_4-p_2p_3}(l_4r_4)-\frac{p_1p_3}{p_1p_4-p_2p_3}(l_1r_2)-\frac{p_2p_3}{p_1p_4-p_2p_3}(l_1r_4)\\
&\quad -\frac{p_3^2}{p_1p_4-p_2p_3}(l_2r_2)-\frac{p_3p_4}{p_1p_4-p_2p_3}(l_2r_4)
\end{aligned}
$$

$\Longrightarrow$

$$
\begin{aligned}
m_2 &\overset{(8)}{\equiv} l_1r_2 + \frac{p_2}{p_1}(l_1r_4 - m_4) + \frac{p_3}{p_1}(l_2r_2) + \frac{p_4}{p_1}(l_2r_4) \\
&\overset{(9)}{\equiv} l_1r_2 + \frac{p_2}{p_1}(l_1r_4) + \frac{p_3}{p_1}(l_2r_2) + \frac{p_4}{p_1}(l_2r_4) - \frac{p_2}{p_1}\cdot\frac{1}{p_1p_4 - p_2p_3}\cdot\Big(p_1^2(l_3r_2) + p_1p_2(l_3r_4) + p_1p_3(l_4r_2) \\
&\quad + p_1p_4(l_4r_4) - p_1p_3(l_1r_2) - p_2p_3(l_1r_4) - p_3^2(l_2r_2) - p_3p_4(l_2r_4)\Big) \\
&\equiv l_1r_2 + \frac{p_2}{p_1}(l_1r_4) + \frac{p_3}{p_1}(l_2r_2) + \frac{p_4}{p_1}(l_2r_4) + \frac{1}{p_1p_4 - p_2p_3}\cdot\Big(-p_1p_2(l_3r_2) - p_2^2(l_3r_4) - p_2p_3(l_4r_2) \\
&\quad - p_2p_4(l_4r_4) + p_2p_3(l_1r_2) + \frac{p_2^2p_3}{p_1}(l_1r_4) + \frac{p_2p_3^2}{p_1}(l_2r_2) + \frac{p_2p_3p_4}{p_1}(l_2r_4)\Big) \\
&\equiv (1 + \frac{p_2p_3}{p_1p_4 - p_2p_3})(l_1r_2) + \frac{p_2}{p_1}(1 + \frac{p_2p_3}{p_1p_4 - p_2p_3})(l_1r_4) + \frac{p_3}{p_1}(1 + \frac{p_2p_3}{p_1p_4 - p_2p_3})(l_2r_2) \\
&\quad + \frac{p_4}{p_1}(1 + \frac{p_2p_3}{p_1p_4 - p_2p_3})(l_2r_4) - \frac{p_1p_2}{p_1p_4 - p_2p_3}(l_3r_2) - \frac{p_2^2}{p_1p_4 - p_2p_3}(l_3r_4) - \frac{p_2p_3}{p_1p_4 - p_2p_3}(l_4r_2) \\
&\quad - \frac{p_2p_4}{p_1p_4 - p_2p_3}(l_4r_4) \\
&\equiv \frac{p_1p_4}{p_1p_4 - p_2p_3}(l_1r_2) + \frac{p_2}{p_1}\frac{p_1p_4}{p_1p_4 - p_2p_3}(l_1r_4) + \frac{p_3}{p_1}\frac{p_1p_4}{p_1p_4 - p_2p_3}(l_2r_2) + \frac{p_4}{p_1}\frac{p_1p_4}{p_1p_4 - p_2p_3}(l_2r_4) \\
&\quad - \frac{p_1p_2}{p_1p_4 - p_2p_3}(l_3r_2) - \frac{p_2^2}{p_1p_4 - p_2p_3}(l_3r_4) - \frac{p_2p_3}{p_1p_4 - p_2p_3}(l_4r_2) - \frac{p_2p_4}{p_1p_4 - p_2p_3}(l_4r_4) \\
&\equiv \frac{p_1p_4}{p_1p_4 - p_2p_3}(l_1r_2) + \frac{p_2p_4}{p_1p_4 - p_2p_3}(l_1r_4) + \frac{p_3p_4}{p_1p_4 - p_2p_3}(l_2r_2) + \frac{p_4^2}{p_1p_4 - p_2p_3}(l_2r_4) \\
&\quad - \frac{p_1p_2}{p_1p_4 - p_2p_3}(l_3r_2) - \frac{p_2^2}{p_1p_4 - p_2p_3}(l_3r_4) - \frac{p_2p_3}{p_1p_4 - p_2p_3}(l_4r_2) - \frac{p_2p_4}{p_1p_4 - p_2p_3}(l_4r_4)
\end{aligned}
$$

En dus kunnen we m_2 en m_4 ook uitdrukken in termen van p_i, l_i en r_i met $i \in \{1, 2, 3, 4\}$.

Nu kunnen we dus concluderen dat $K_l \cdot P \cdot K_r \equiv P \cdot M \pmod{29}$, voor een zekere matrix $M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$ met

$$
\begin{aligned}
m_1 &\equiv \frac{p_1p_4}{p_1p_4 - p_2p_3}(l_1r_1) + \frac{p_2p_4}{p_1p_4 - p_2p_3}(l_1r_3) + \frac{p_3p_4}{p_1p_4 - p_2p_3}(l_2r_1) + \frac{p_4^2}{p_1p_4 - p_2p_3}(l_2r_3) \\
&\quad - \frac{p_1p_2}{p_1p_4 - p_2p_3}(l_3r_1) - \frac{p_2^2}{p_1p_4 - p_2p_3}(l_3r_3) - \frac{p_2p_3}{p_1p_4 - p_2p_3}(l_4r_1) - \frac{p_2p_4}{p_1p_4 - p_2p_3}(l_4r_3) \\
m_2 &\equiv \frac{p_1p_4}{p_1p_4 - p_2p_3}(l_1r_2) + \frac{p_2p_4}{p_1p_4 - p_2p_3}(l_1r_4) + \frac{p_3p_4}{p_1p_4 - p_2p_3}(l_2r_2) + \frac{p_4^2}{p_1p_4 - p_2p_3}(l_2r_4) \\
&\quad - \frac{p_1p_2}{p_1p_4 - p_2p_3}(l_3r_2) - \frac{p_2^2}{p_1p_4 - p_2p_3}(l_3r_4) - \frac{p_2p_3}{p_1p_4 - p_2p_3}(l_4r_2) - \frac{p_2p_4}{p_1p_4 - p_2p_3}(l_4r_4) \\
m_3 &\equiv \frac{p_1^2}{p_1p_4 - p_2p_3}(l_3r_1) + \frac{p_1p_2}{p_1p_4 - p_2p_3}(l_3r_3) + \frac{p_1p_3}{p_1p_4 - p_2p_3}(l_4r_1) + \frac{p_1p_4}{p_1p_4 - p_2p_3}(l_4r_3) \\
&\quad - \frac{p_1p_3}{p_1p_4 - p_2p_3}(l_1r_1) - \frac{p_2p_3}{p_1p_4 - p_2p_3}(l_1r_3) - \frac{p_3^2}{p_1p_4 - p_2p_3}(l_2r_1) - \frac{p_3p_4}{p_1p_4 - p_2p_3}(l_2r_3)
\end{aligned}
$$

$$\begin{aligned} m_4 \equiv\ & \frac{p_1^2}{p_1p_4 - p_2p_3}(l_3r_2) + \frac{p_1p_2}{p_1p_4 - p_2p_3}(l_3r_4) + \frac{p_1p_3}{p_1p_4 - p_2p_3}(l_4r_2) + \frac{p_1p_4}{p_1p_4 - p_2p_3}(l_4r_4) \\ & - \frac{p_1p_3}{p_1p_4 - p_2p_3}(l_1r_2) - \frac{p_2p_3}{p_1p_4 - p_2p_3}(l_1r_4) - \frac{p_3^2}{p_1p_4 - p_2p_3}(l_2r_2) - \frac{p_3p_4}{p_1p_4 - p_2p_3}(l_2r_4) \end{aligned}$$

Opmerking 2.2. In de berekening van m_1, m_2, m_3, m_4 zijn we er van uitgegaan dat $p_i \neq 0$ voor alle $i \in \{1,2,3,4\}$ en dat $\det(P) = p_1p_4 - p_2p_3 \neq 0$. Dit hoeft echter helemaal niet te gelden, want we willen elke mogelijke plaintext kunnen versturen, dus bijvoorbeeld ook $P = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Gelukkig mogen we dit door de vingers zien, omdat we onze zonde kunnen goedpraten doordat we de linker- en rechterleden hierboven kunnen vermenigvuldigen met $p_1p_4 - p_2p_3$, zodat we niet meer door 0 delen. Het gevolg hiervan is dat we M wel met behulp van Gauss-eliminatie kunnen bepalen, maar M is niet meer uniek vastgelegd. Als $p_i = 0$ voor een zekere $i \in \{1,2,3,4\}$ of als $\det(P) = 0$, dan moeten we dus oppassen en kunnen we m_1, m_2, m_3, m_4 niet op bovenstaande wijze berekenen. ◁

Voorbeeld 2.3. Neem $K_l = K_r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ en veronderstel dat $\det(P) = p_1p_4 - p_2p_3 = 0$. Dan volgt uit (1)–(4) dat moet gelden (mod 29):

$$\begin{aligned} p_1 &\equiv p_1m_1 + p_2m_3 \\ p_2 &\equiv p_1m_2 + p_2m_4 \\ p_3 &\equiv p_3m_1 + p_4m_3 \\ p_4 &\equiv p_3m_2 + p_4m_4 \end{aligned}$$

Nu voldoet $M = \begin{pmatrix} m_1 & m_2 \\ \frac{p_1}{p_2} - \frac{p_1}{p_2}m_1 & 1 - \frac{p_1}{p_2}m_2 \end{pmatrix} = \begin{pmatrix} m_1 & m_2 \\ \frac{p_3}{p_4} - \frac{p_3}{p_4}m_1 & 1 - \frac{p_3}{p_4}m_2 \end{pmatrix}$ voor willekeurige m_1 en m_2. Er bestaan dus meerdere geldige oplossingen. ◁

Welke conclusie kunnen we verbinden aan het feit dat m_1, m_2, m_3, m_4 zijn uit te drukken in termen van p_i, l_i en r_i met $i \in \{1,2,3,4\}$?

Stelling 2.4. *Matrix M is niet uniek vastgelegd.*
Bewijs: Als $\det(P) = 0$, dan ligt M niet vast, zoals we hierboven reeds gezien hadden. Als $\det(P) \neq 0$, dan volgt uit de vergelijkingen voor m_1, m_2, m_3, m_4 dat al deze m_i afhankelijk zijn van p_i, l_i en r_i met $i \in \{1,2,3,4\}$. Matrix M is dus afhankelijk van matrix P. Maar P is onze plaintext en deze verandert per te coderen boodschap en dus is M ook voor elke boodschap anders. ◁

2.4 Het kraken van de sleutels

Zoals eerder vermeld is de Hill-cipher kwetsbaar tegen plaintext attacks. We zijn benieuwd of onze "geüpgradede" Hill-cipher wél bestand is tegen zulk geweld.

Om de sleutels K_l en K_r te kunnen achterhalen is het nodig dat we l_i en r_i voor alle $i \in \{1,2,3,4\}$ te weten komen. Omdat we tot nu toe echter alleen met combinaties l_ir_j hebben gewerkt, moeten we ons eerst toespitsen op deze paren l_ir_j voor alle $i,j \in \{1,2,3,4\}$. We zullen hiertoe twee verschillende methoden geven om de sleutels K_l en K_r te kunnen achterhalen. Maar eerst nog even kort een lemma dat we nodig zullen gaan hebben.

Lemma 2.5. *Als de sleutels K_l en K_r bekend zijn, dan kunnen er sleutels $\overline{K_l}$ en $\overline{K_r}$ met $\overline{K_l} \neq K_l$ en $\overline{K_r} \neq K_r$ worden gevonden, zodanig dat $K_l \cdot P \cdot K_r \equiv \overline{K_l} \cdot P \cdot \overline{K_r}$ (mod 29) voor alle P.*
Bewijs: We rekenen modulo 29, dus elk getal $x \in \{1, 2, 3, ..., 28\}$ heeft een inverse modulo 29. Daarom volgt, mits $l_1 \neq 0$:

$$\begin{aligned}
K_l \cdot P \cdot K_r &\equiv \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \\
&\equiv l_1 \begin{pmatrix} 1 & \frac{l_2}{l_1} \\ \frac{l_3}{l_1} & \frac{l_4}{l_1} \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \\
&\equiv \begin{pmatrix} 1 & \frac{l_2}{l_1} \\ \frac{l_3}{l_1} & \frac{l_4}{l_1} \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} l_1 r_1 & l_1 r_2 \\ l_1 r_3 & l_1 r_4 \end{pmatrix} \\
&\equiv \begin{pmatrix} \overline{l_1} & \overline{l_2} \\ \overline{l_3} & \overline{l_4} \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} \overline{r_1} & \overline{r_2} \\ \overline{r_3} & \overline{r_4} \end{pmatrix} \\
&\equiv \overline{K_l} \cdot P \cdot \overline{K_r}
\end{aligned}$$

Als $l_1 = 0$ dan kunnen we hetzelfde trucje uithalen met l_2. (Als $l_1 = 0$ dan $l_2 \neq 0$, want anders is $\det(K_l) = 0$ en dat is verboden.) ◁

Gevolg 2.6. *Er zijn minstens 28 verschillende combinaties K_l, K_r zodanig dat $K_{l_u} \cdot P \cdot K_{r_u} \equiv K_{l_v} \cdot P \cdot K_{r_v}$ voor alle $u, v \in \{1, 2, ..., 28\}$ en voor alle P.*
Bewijs: Als $l_{1_u} \neq 0$ dan kunnen we K_{l_u} met een constante $d \in \{1, 2, 3, ..., 28\}$ en K_{r_u} met $\frac{1}{d}$ (mod 29) vermenigvuldigen, zodat l_{1_u} de waarden $\{1, 2, ..., 28\}$ kan aannemen:

$$\begin{aligned}
K_{l_u} \cdot P \cdot K_{r_u} &\equiv \begin{pmatrix} l_{1_u} & l_{2_u} \\ l_{3_u} & l_{4_u} \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} r_{1_u} & r_{2_u} \\ r_{3_u} & r_{4_u} \end{pmatrix} \\
&\equiv d \cdot \frac{1}{d} \cdot \begin{pmatrix} l_{1_u} & l_{2_u} \\ l_{3_u} & l_{4_u} \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} r_{1_u} & r_{2_u} \\ r_{3_u} & r_{4_u} \end{pmatrix} \\
&\equiv \begin{pmatrix} d\, l_{1_u} & d\, l_{2_u} \\ d\, l_{3_u} & d\, l_{4_u} \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} \frac{1}{d}\, r_{1_u} & \frac{1}{d}\, r_{2_u} \\ \frac{1}{d}\, r_{3_u} & \frac{1}{d}\, r_{4_u} \end{pmatrix} \\
&\equiv \begin{pmatrix} l_{1_v} & l_{2_v} \\ l_{3_v} & l_{4_v} \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} r_{1_v} & r_{2_v} \\ r_{3_v} & r_{4_v} \end{pmatrix} \\
&\equiv K_{l_v} \cdot P \cdot K_{r_v}
\end{aligned}$$

Als $l_{1_u} = 0$ dan geldt hetzelfde argument voor l_{2_u}.
Zo krijgen we 28 verschillende combinaties K_l, K_r. Elke combinatie verstuurt een willekeurige plaintext naar een en dezelfde ciphertext. ◁

Opmerking 2.7. We willen de lezer erop attenderen dat het bovenstaande foefje niet alleen voor één bepaalde plaintext P opgaat, maar voor álle boodschappen P. We hebben in ons bewijs namelijk gebruikgemaakt van een gegeneraliseerde $P = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix}$. ◁

Laat het kraken beginnen!

2.4.1 Methode 1

Ter herinnering uit hoofdstuk 1 herhalen we even dat

$$\begin{pmatrix} p_1(l_1r_1)+p_2(l_1r_3)+p_3(l_2r_1)+p_4(l_2r_3) & p_1(l_1r_2)+p_2(l_1r_4)+p_3(l_2r_2)+p_4(l_2r_4) \\ p_1(l_3r_1)+p_2(l_3r_3)+p_3(l_4r_1)+p_4(l_4r_3) & p_1(l_3r_2)+p_2(l_3r_4)+p_3(l_4r_2)+p_4(l_4r_4) \end{pmatrix} \equiv \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$

Net zoals bij de orginele Hill-cipher kiezen we eerst enkele onafhankelijke boodschappen uit en we kijken wat de bijbehorende ciphertext bij elke plaintext is. Dan kennen we namelijk p_i en c_i voor alle $i \in \{1,2,3,4\}$ en dus kunnen we c_1, c_2, c_3 en c_4 uitdrukken in termen van l_ir_j.

Ter illustratie zullen we er voor kiezen om te werken met de volgende vier boodschappen. Merk op dat we specifiek voor vier boodschappen kiezen, omdat er zestien verschillende paren l_ir_j zijn en bij vier boodschappen krijgen we zestien c_i'tjes. Met andere woorden: we krijgen een stelsel van zestien vergelijkingen met zestien onbekenden. De vier boodschappen die we uitkiezen definiëren we als volgt:

$$P^\alpha := \begin{pmatrix} p_1^\alpha & p_2^\alpha \\ p_3^\alpha & p_4^\alpha \end{pmatrix},\ P^\beta := \begin{pmatrix} p_1^\beta & p_2^\beta \\ p_3^\beta & p_4^\beta \end{pmatrix},\ P^\gamma := \begin{pmatrix} p_1^\gamma & p_2^\gamma \\ p_3^\gamma & p_4^\gamma \end{pmatrix},\ P^\delta := \begin{pmatrix} p_1^\delta & p_2^\delta \\ p_3^\delta & p_4^\delta \end{pmatrix}.$$

We kiezen nu

$$P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ P^\gamma = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ P^\delta = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Het is eenvoudig aan te tonen dat deze vier matrices onafhankelijk zijn:

$$\lambda_1 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \lambda_4 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Longrightarrow \qquad \lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 0$$

En dus zijn de matrices onafhankelijk.

Deze vier boodschappen gekozen hebbende zien we, met behulp van de vergelijkingen uit het begin van deze paragraaf, dat hierbij de volgende ciphertextvergelijkingen horen modulo 29:

$$\begin{aligned} c_1^\alpha &\equiv l_1r_1 \\ c_2^\alpha &\equiv l_1r_2 \\ c_3^\alpha &\equiv l_3r_1 \\ c_4^\alpha &\equiv l_3r_2 \end{aligned}$$

$$\begin{aligned} c_1^\beta &\equiv l_1r_3 \\ c_2^\beta &\equiv l_1r_4 \\ c_3^\beta &\equiv l_3r_3 \\ c_4^\beta &\equiv l_3r_4 \end{aligned}$$

$$\begin{aligned} c_1^\gamma &\equiv l_2 r_1 \\ c_2^\gamma &\equiv l_2 r_2 \\ c_3^\gamma &\equiv l_4 r_1 \\ c_4^\gamma &\equiv l_4 r_2 \end{aligned}$$

$$\begin{aligned} c_1^\delta &\equiv l_2 r_3 \\ c_2^\delta &\equiv l_2 r_4 \\ c_3^\delta &\equiv l_4 r_3 \\ c_4^\delta &\equiv l_4 r_4 \end{aligned}$$

We hebben nu alle zestien paren $l_i r_j$ uitgedrukt in $c_i^k \pmod{29}$ met $i \in \{1,2,3,4\}$ en $k \in \{\alpha, \beta, \gamma, \delta\}$. Het ligt nu in de lijn der verwachting dat we l_i en r_i voor alle $i \in \{1,2,3,4\}$ kunnen uitdrukken in termen die we kennen (zoals c_i^k). Helaas blijkt dit echter een onmogelijke opgave te zijn; we blijven altijd ergens met l_i'tjes en/of r_i'tjes zitten op plekken waar we ze liever niet tegenkomen. Ondanks het feit dat dit wel eens, met het oog op vijand Eve, zeer gunstig uit zou kunnen pakken voor onze Hill-cipher, zijn de sleutels toch vrij eenvoudig te achterhalen. Althans, Eve kan sleutels $\overline{K_l}$ en $\overline{K_r}$ vinden die exact dezelfde werking hebben als K_l en K_r (maar toch verschillend kunnen zijn). Dit betekent dat voor elke P geldt: $\overline{K_l} \cdot P \cdot \overline{K_r} \equiv K_l \cdot P \cdot K_r \pmod{29}$. Waarom deze $\overline{K_l}$ en $\overline{K_r}$ bestaan volgt uit Lemma 2.5. Eve weet namelijk dát er K_l en K_r bestaan, dus bestaan er ook $\overline{K_l}$ en $\overline{K_r}$.

De zestien vergelijkingen voor c_i^k hierboven veranderen nu ook automatisch:

$$\begin{aligned} c_1^\alpha &\equiv \overline{l_1}\,\overline{r_1} \\ c_2^\alpha &\equiv \overline{l_1}\,\overline{r_2} \\ c_3^\alpha &\equiv \overline{l_3}\,\overline{r_1} \\ c_4^\alpha &\equiv \overline{l_3}\,\overline{r_2} \end{aligned}$$

$$\begin{aligned} c_1^\beta &\equiv \overline{l_1}\,\overline{r_3} \\ c_2^\beta &\equiv \overline{l_1}\,\overline{r_4} \\ c_3^\beta &\equiv \overline{l_3}\,\overline{r_3} \\ c_4^\beta &\equiv \overline{l_3}\,\overline{r_4} \end{aligned}$$

$$\begin{aligned} c_1^\gamma &\equiv \overline{l_2}\,\overline{r_1} \\ c_2^\gamma &\equiv \overline{l_2}\,\overline{r_2} \\ c_3^\gamma &\equiv \overline{l_4}\,\overline{r_1} \\ c_4^\gamma &\equiv \overline{l_4}\,\overline{r_2} \end{aligned}$$

$$\begin{aligned} c_1^\delta &\equiv \overline{l_2}\,\overline{r_3} \\ c_2^\delta &\equiv \overline{l_2}\,\overline{r_4} \\ c_3^\delta &\equiv \overline{l_4}\,\overline{r_3} \\ c_4^\delta &\equiv \overline{l_4}\,\overline{r_4} \end{aligned}$$

We kunnen dus $\overline{l_1} = 1$ kiezen en dan liggen de overige $\overline{l_i}$, $\overline{r_i}$ vast volgens de c_i^k die we hierboven hebben uitgedrukt in $\overline{l_i}$, $\overline{r_i}$. En hiermee zijn $\overline{K_l}$ en $\overline{K_r}$ bepaald.

Voorbeeld 2.8. We nemen $K_l = \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix}$ en $K_r = \begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix}$, maar Eve kent deze sleutels niet. (Merk op dat $\det(K_l) \neq 0$ en $\det(K_r) \neq 0$.) Voor een plaintext attack vult Eve achtereenvolgens de matrices

$$P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ P^\gamma = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ P^\delta = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

in in $K_l \cdot P \cdot K_r$ en het blijkt dat ze respectievelijk de volgende matrices (modulo 29) als ciphertext terugkrijgt:

$$\begin{aligned}
C^\alpha &\equiv \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix} \equiv \begin{pmatrix} 20 & 5 \\ 23 & 13 \end{pmatrix} \\
C^\beta &\equiv \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix} \equiv \begin{pmatrix} 17 & 22 \\ 21 & 5 \end{pmatrix} \\
C^\gamma &\equiv \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix} \equiv \begin{pmatrix} 3 & 8 \\ 13 & 25 \end{pmatrix} \\
C^\delta &\equiv \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix} \equiv \begin{pmatrix} 4 & 12 \\ 27 & 23 \end{pmatrix}
\end{aligned}$$

Dus krijgt Eve:

$$\begin{aligned}
c_1^\alpha &\equiv l_1 r_1 \equiv 20 \\
c_2^\alpha &\equiv l_1 r_2 \equiv 5 \\
c_3^\alpha &\equiv l_3 r_1 \equiv 23 \\
c_4^\alpha &\equiv l_3 r_2 \equiv 13
\end{aligned}$$

$$\begin{aligned}
c_1^\beta &\equiv l_1 r_3 \equiv 17 \\
c_2^\beta &\equiv l_1 r_4 \equiv 22 \\
c_3^\beta &\equiv l_3 r_3 \equiv 21 \\
c_4^\beta &\equiv l_3 r_4 \equiv 5
\end{aligned}$$

$$\begin{aligned}
c_1^\gamma &\equiv l_2 r_1 \equiv 3 \\
c_2^\gamma &\equiv l_2 r_2 \equiv 8 \\
c_3^\gamma &\equiv l_4 r_1 \equiv 13 \\
c_4^\gamma &\equiv l_4 r_2 \equiv 25
\end{aligned}$$

$$\begin{aligned}
c_1^\delta &\equiv l_2 r_3 \equiv 4 \\
c_2^\delta &\equiv l_2 r_4 \equiv 12 \\
c_3^\delta &\equiv l_4 r_3 \equiv 27 \\
c_4^\delta &\equiv l_4 r_4 \equiv 23
\end{aligned}$$

Omdat $l_1 r_1 \equiv 20 \not\equiv 0$, volgt dat $l_1 \neq 0$. Eve kiest dus $\overline{l_1} = 1$. Dan volgt modulo 29:

$$\overline{r_1} = 20 \ , \ \overline{r_2} = 5 \ , \ \overline{r_3} = 17 \ , \ \overline{r_4} = 22 \ .$$

Er moet nu gelden:

$$\begin{aligned} l_2 r_1 \equiv \overline{l_2}\ \overline{r_1} \equiv \overline{l_2} \cdot 20 \equiv 3 \quad &\Longrightarrow \quad \overline{l_2} \equiv 19 \\ l_3 r_1 \equiv \overline{l_3}\ \overline{r_1} \equiv \overline{l_3} \cdot 20 \equiv 23 \quad &\Longrightarrow \quad \overline{l_3} \equiv 20 \\ l_4 r_1 \equiv \overline{l_4}\ \overline{r_1} \equiv \overline{l_4} \cdot 20 \equiv 13 \quad &\Longrightarrow \quad \overline{l_4} \equiv 5 \end{aligned}$$

En dus krijgt ze:

$$\overline{K_l} = \begin{pmatrix} 1 & 19 \\ 20 & 5 \end{pmatrix} \ , \ \overline{K_r} = \begin{pmatrix} 20 & 5 \\ 17 & 22 \end{pmatrix} \ .$$

Zonder enige kennis van de orginele sleutels K_l en K_r is Eve er toch in geslaagd om sleutels $\overline{K_l}$ en $\overline{K_r}$ te vinden die hetzelfde uithalen met een plaintext P als de oorspronkelijke sleutels. In het vervolg kan Eve dus van elke gecodeerde boodschap C de plaintext P achterhalen! $\lhd$

Samenvatting 2.9. Samenvattend kunnen we concluderen dat Methode 1 bestaat uit de volgende handelingen:

- Eve voert een plaintext attack uit: ze neemt de vier onafhankelijke matrices

  $$P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ P^\gamma = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \ P^\delta = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

  en kijkt wat de bijbehorende gecodeerde boodschappen C^α, C^β, C^γ, C^δ zijn; hieruit verkrijgt zij zestien vergelijkingen.

- Zij kiest $\overline{l_1} = 1$, waardoor de overige zeven $\overline{l_i}$, $\overline{r_i}$ vast komen te liggen. Deze kan Eve uitrekenen, zodat zij $\overline{K_l}$ en $\overline{K_r}$ kan bepalen.

- Nu kan Eve bij elke ciphertext C de bijbehorende plaintext $P \equiv \overline{K_l}^{-1} \cdot C \cdot \overline{K_r}^{-1} \pmod{29}$ uitrekenen.

$\lhd$

Opmerking 2.10. In (de uitleg en samenvatting van) Methode 1 hebben we steeds gesproken over *de* vier matrices

$$P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ P^\gamma = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \ P^\delta = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \ .$$

We hebben deze vier onafhankelijke matrices voor onze plaintext attack gekozen omdat dit verreweg het handigst is om mee te rekenen. Echter volstaat elke combinatie van vier onafhankelijke matrices

$$P^\alpha = \begin{pmatrix} p_1^\alpha & p_2^\alpha \\ p_3^\alpha & p_4^\alpha \end{pmatrix}, \ P^\beta = \begin{pmatrix} p_1^\beta & p_2^\beta \\ p_3^\beta & p_4^\beta \end{pmatrix}, \ P^\gamma = \begin{pmatrix} p_1^\gamma & p_2^\gamma \\ p_3^\gamma & p_4^\gamma \end{pmatrix}, \ P^\delta = \begin{pmatrix} p_1^\delta & p_2^\delta \\ p_3^\delta & p_4^\delta \end{pmatrix}$$

met p_i^α, p_i^β, p_i^γ, $p_i^\delta \in \{0, 1, 2, ..., 28\}$ voor alle $i \in \{1, 2, 3, 4\}$, want elke matrix is een lineaire combinatie van de vier onafhankelijke matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \ .$$

Bijvoorbeeld:

$$P^\alpha = \begin{pmatrix} p_1^\alpha & p_2^\alpha \\ p_3^\alpha & p_4^\alpha \end{pmatrix} = p_1^\alpha \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + p_2^\alpha \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + p_3^\alpha \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + p_4^\alpha \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

De clou waarom elke vier onafhankelijke boodschappen P^α, P^β, P^γ, P^δ gekozen kunnen worden zit hem erin dat de vier bijbehorende gecodeerde boodschappen $P^\alpha \cdot K \equiv C^\alpha$, $P^\beta \cdot K \equiv C^\beta$, $P^\gamma \cdot K \equiv C^\gamma$, $P^\delta \cdot K \equiv C^\delta \pmod{29}$ onderling ook weer onafhankelijk zijn. De boodschappen worden namelijk vermenigvuldigd met een vaste matrix K. Vanwege de onafhankelijkheid van C^α, C^β, C^γ en C^δ kan Eve de vergelijkingen die zij hieruit verkrijgt oplossen. ◁

Opmerking 2.11. In Methode 1 maakt Eve zoals gezegd gebruik van een plaintext attack. In de vorige opmerking hebben we gezien dat Eve met elk viertal onafhankelijke matrices de encryptiesleutels kan achterhalen; welke matrices dit zijn maakt (afgezien van het rekenwerk) niets uit. Deze vorm van een plaintext attack noemen we een *known-plaintext attack*. Bij Methode 2 zullen we nog een ander soort plaintext attack tegenkomen. ◁

2.4.2 Methode 2

De tweede methode is erop gebaseerd om de gecodeerde boodschap$K_l \cdot P \cdot K_r$ te schrijven als een oorspronkelijke Hill-cipher. In paragraaf 2.3 hebben we echter aangetoond dat dit onmogelijk is. Vandaar dat we de boel enigszins aanpassen: we gaan niet meer op zoek naar een vaste matrix M zodanig dat geldt $K_l \cdot P \cdot K_r \equiv P \cdot M \pmod{29}$ voor alle P (deze M bestond namelijk niet), maar we willen nu een vaste matrix M kiezen zodanig dat $K_l \cdot P \cdot K_r \equiv Q \cdot M \pmod{29}$ voor alle Q. Hierbij moeten we meteen melden dat deze Q van P af mag en zal hangen. De truc is nu om deze Q en M op een slimme manier te kiezen.

Om meteen met de deur in huis te vallen: kies Q en M als volgt (mod 29):

$$\begin{aligned} Q &\equiv K_l \cdot P \cdot K_l^{-1} \\ M &\equiv K_l \cdot K_r \end{aligned}$$

Matrix P heeft dus een basistransformatie ondergaan (Q is geconjugeerd met P) en M is nu een sleutel van de oorspronkelijke Hill-cipher. We zien dat voor de zojuist gekozen Q en M geldt (mod 29):

$$\begin{aligned} Q \cdot M &\equiv K_l \cdot P \cdot K_l^{-1} \cdot K_l \cdot K_r \\ &\equiv K_l \cdot P \cdot K_r \end{aligned}$$

Precies datgene wat we wilden dus. We, dat wil zeggen Eve, kennen M bij voorbaat nog niet. Maar het mooie (althans, mooi voor Eve, want Alice en Bob staan er niet om te springen) is dat Eve met slechts één plaintext attack M kan achterhalen. Vul namelijk maar $P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in in $K_l \cdot P \cdot K_r$ en $M \equiv K_l \cdot K_r \pmod{29}$ rolt uit onze snoepautomaat!

Nu moeten we nog Q bepalen. Uitschrijven levert een eerste inzicht:

$$\begin{aligned} Q &\equiv K_l \cdot P \cdot K_l^{-1} \\ &\equiv \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix}^{-1} \\ &\equiv \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \cdot \frac{1}{l_1 l_4 - l_2 l_3} \cdot \begin{pmatrix} l_4 & -l_2 \\ -l_3 & l_1 \end{pmatrix} \end{aligned}$$

$$
\begin{aligned}
&\equiv \frac{1}{l_1l_4 - l_2l_3} \cdot \begin{pmatrix} l_1p_1 + l_2p_3 & l_1p_2 + l_2p_4 \\ l_3p_1 + l_4p_3 & l_3p_2 + l_4p_4 \end{pmatrix} \begin{pmatrix} l_4 & -l_2 \\ -l_3 & l_1 \end{pmatrix} \\
&\equiv \frac{1}{l_1l_4 - l_2l_3} \cdot \begin{pmatrix} (l_1p_1 + l_2p_3)l_4 - (l_1p_2 + l_2p_4)l_3 & -(l_1p_1 + l_2p_3)l_2 + (l_1p_2 + l_2p_4)l_1 \\ (l_3p_1 + l_4p_3)l_4 - (l_3p_2 + l_4p_4)l_3 & -(l_3p_1 + l_4p_3)l_2 + (l_3p_2 + l_4p_4)l_1 \end{pmatrix} \\
&\equiv \frac{1}{l_1l_4 - l_2l_3} \cdot \begin{pmatrix} p_1(l_1l_4) - p_2(l_1l_3) + p_3(l_2l_4) - p_4(l_2l_3) & -p_1(l_1l_2) + p_2(l_1^2) - p_3(l_2^2) + p_4(l_1l_2) \\ p_1(l_3l_4) - p_2(l_3^2) + p_3(l_4^2) - p_4(l_3l_4) & -p_1(l_2l_3) + p_2(l_1l_3) - p_3(l_2l_4) + p_4(l_1l_4) \end{pmatrix}
\end{aligned}
$$

Zoals we hebben gezien kan Eve met een enkele plaintext attack de matrix M bepalen. Zij komt Q hiermee echter nog niet te weten, omdat Q alleen van l_i met $i \in \{1, 2, 3, 4\}$ afhangt en niet van combinaties l_ir_j met $i, j \in \{1, 2, 3, 4\}$, zoals M.

Bij een gegeven boodschap P kan Eve de matrix Q wel als volgt berekenen. We hebben gezien dat $K_l \cdot P \cdot K_r \equiv Q \cdot M \pmod{29}$ en anderzijds geldt uiteraard $K_l \cdot P \cdot K_r \equiv C \pmod{29}$. Dus volgt modulo 29:

$$
\begin{aligned}
Q &\equiv K_l \cdot P \cdot K_r \cdot M^{-1} \\
&\equiv C \cdot M^{-1} \\
&\equiv C \cdot (K_l \cdot K_r)^{-1}
\end{aligned}
$$

We zien het volgende gebeuren: als Eve een plaintext P^* kiest, dan weet ze wat C^* is en dus kan ze Q^* bepalen, want M^{-1} bestaat vanwege $\det(K_l) \neq 0$ en $\det(K_r) \neq 0$.

Theoretisch zou Eve, net zoals ze in Methode 1 heeft gedaan, weer de vier onafhankelijke matrices

$$
P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ P^\gamma = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ P^\delta = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}
$$

kunnen kiezen en de bijbehorende matrices Q^α, Q^β, Q^γ en Q^δ berekenen modulo 29:

$$
\begin{aligned}
P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &\implies Q^\alpha \equiv \frac{1}{l_1l_4 - l_2l_3} \begin{pmatrix} l_1l_4 & -l_1l_2 \\ l_3l_4 & -l_2l_3 \end{pmatrix} \\
P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} &\implies Q^\beta \equiv \frac{1}{l_1l_4 - l_2l_3} \begin{pmatrix} -l_1l_3 & l_1^2 \\ -l_3^2 & l_1l_3 \end{pmatrix} \\
P^\gamma = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} &\implies Q^\gamma \equiv \frac{1}{l_1l_4 - l_2l_3} \begin{pmatrix} l_2l_4 & -l_2^2 \\ l_4^2 & -l_2l_4 \end{pmatrix} \\
P^\delta = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} &\implies Q^\delta \equiv \frac{1}{l_1l_4 - l_2l_3} \begin{pmatrix} -l_2l_3 & l_1l_2 \\ -l_3l_4 & l_1l_4 \end{pmatrix}
\end{aligned}
$$

Helaas heeft Eve niet zoveel aan deze kennis van Q^k met $k \in \{\alpha, \beta, \gamma, \delta\}$, omdat ze $\det(K_l) = l_1l_4 - l_2l_3$ niet kent. Hierdoor kan ze dus de combinaties l_il_j met $i, j \in \{1, 2, 3, 4\}$ niet bepalen, laat staan de afzonderlijke l_i met $i \in \{1, 2, 3, 4\}$. Gelukkig voor Eve kan zij zich uit deze penibele situatie redden. Als we de vergelijkingen echter op een andere manier opschrijven, dan lukt het wél:

$$
Q \equiv K_l \cdot P \cdot K_l^{-1} \implies Q \cdot K_l \equiv K_l \cdot P
$$

Kiezen we nu de matrices met plaintext

$$
P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},
$$

dan krijgen we vergelijkingen met vier onbekenden l_1, l_2, l_3, l_4 waarmee we zodanig kunnen goochelen dat we K_l kunnen uitdrukken in termen van l_1:

$$\begin{aligned}
P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad &\Longrightarrow \quad Q^\alpha \cdot K_l \equiv Q^\alpha \cdot \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \equiv \begin{pmatrix} l_1 & 0 \\ l_3 & 0 \end{pmatrix} \\
&\Longrightarrow \quad q_1^\alpha l_1 + q_2^\alpha l_3 \equiv l_1 \\
&\qquad\quad\; q_1^\alpha l_2 + q_2^\alpha l_4 \equiv 0 \\
&\qquad\quad\; q_3^\alpha l_1 + q_4^\alpha l_3 \equiv l_3 \\
&\qquad\quad\; q_3^\alpha l_2 + q_4^\alpha l_4 \equiv 0 \\
P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad &\Longrightarrow \quad Q^\beta \cdot K_l \equiv Q^\beta \cdot \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \equiv \begin{pmatrix} 0 & l_1 \\ 0 & l_3 \end{pmatrix} \\
&\Longrightarrow \quad q_1^\beta l_1 + q_2^\beta l_3 \equiv 0 \\
&\qquad\quad\; q_1^\beta l_2 + q_2^\beta l_4 \equiv l_1 \\
&\qquad\quad\; q_3^\beta l_1 + q_4^\beta l_3 \equiv 0 \\
&\qquad\quad\; q_3^\beta l_2 + q_4^\beta l_4 \equiv l_3
\end{aligned}$$

waarbij $Q^\alpha \equiv \begin{pmatrix} q_1^\alpha & q_2^\alpha \\ q_3^\alpha & q_4^\alpha \end{pmatrix}$ en $Q^\beta \equiv \begin{pmatrix} q_1^\beta & q_2^\beta \\ q_3^\beta & q_4^\beta \end{pmatrix}$ door Eve berekend kunnen worden. Merk op dat Eve nu slechts twee(!) P-matrices gebruikt in plaats van vier.

Met behulp van deze acht vergelijkingen kan Eve nu de linkersleutel K_l uitdrukken in termen van l_1, zeg $K_l = \begin{pmatrix} \mu_1 l_1 & \mu_2 l_1 \\ \mu_3 l_1 & \mu_4 l_1 \end{pmatrix}$ voor zekere $\mu_i \in \{0, 1, 2, ..., 28\}$, $i \in \{1, 2, 3, 4\}$ (sterker nog: $\mu_1 = 1$). Voor elke keuze van $l_1 \in \{1, 2, ..., 28\}$ is K_l nu een goede sleutel. Stel Eve kiest $l_1 = 1$ en laat $\overline{K_l}$ de zo ontstane matrix zijn. Zij kent nu zowel $\overline{K_l}$ als $K_l \cdot K_r \pmod{29}$. Hieruit wil zij $\overline{K_r}$ bepalen, zodanig dat $\overline{K_l} \cdot P \cdot \overline{K_r} \equiv K_l \cdot P \cdot K_r \pmod{29}$ voor alle P, waarbij K_l en K_r de oorspronkelijk door Alice en Bob gekozen sleutels zijn. De vraag is nu: hoe kan Eve $\overline{K_r}$ bepalen, zonder dat zij $\overline{K_l} \cdot \overline{K_r} \pmod{29}$ kent?

Stelling 2.12. *Laat K_{l_u}, K_{r_u} respectievelijk K_{l_v}, K_{r_v} met $u, v \in \{1, 2, ..., 28\}$ twee verschillende combinaties van een linker- en een rechtersleutel zijn zodanig dat $K_{l_u} \cdot P \cdot K_{r_u} \equiv K_{l_v} \cdot P \cdot K_{r_v} \pmod{29}$ voor alle P. Dan geldt voor alle P modulo 29:*

$$K_{l_u} \cdot P \cdot K_{l_u}^{-1} \equiv K_{l_v} \cdot P \cdot K_{l_v}^{-1}.$$

Bewijs: Voor alle P geldt:

$$\begin{aligned}
&K_{l_u} \cdot P \cdot K_{r_u} \equiv K_{l_v} \cdot P \cdot K_{r_v} \\
&\overset{P=I}{\Downarrow} \\
&K_{l_u} \cdot K_{r_u} \equiv K_{l_v} \cdot K_{r_v} \\
&\Downarrow \\
&K_{l_u} \cdot K_{r_u} \equiv M \equiv K_{l_v} \cdot K_{r_v} \\
&\Downarrow
\end{aligned}$$

$$K_{l_u} \cdot P \cdot K_{r_u} \equiv K_{l_u} \cdot P \cdot K_{l_u}^{-1} \cdot K_{l_u} \cdot K_{r_u} \equiv K_{l_u} \cdot P \cdot K_{l_u}^{-1} \cdot M$$
$$|||$$
$$K_{l_v} \cdot P \cdot K_{r_v} \equiv K_{l_v} \cdot P \cdot K_{l_v}^{-1} \cdot K_{l_v} \cdot K_{r_v} \equiv K_{l_v} \cdot P \cdot K_{l_v}^{-1} \cdot M$$
$$\Downarrow$$
$$K_{l_u} \cdot P \cdot K_{l_u}^{-1} \equiv K_{l_v} \cdot P \cdot K_{l_v}^{-1}$$

$\lhd$

Terug naar Eve. Zij kent zoals gezegd $\overline{K_l}$ en $K_l \cdot K_r \pmod{29}$. Laat nu $K_l \equiv K_{l_u}, K_r \equiv K_{r_u}, \overline{K_l} \equiv K_{l_v} \pmod{29}$. Dan volgt uit (het bewijs van) Stelling 2.12 dat $K_l \cdot K_r \equiv \overline{K_l} \cdot \overline{K_r} \pmod{29}$. Maar dan kan Eve ook $\overline{K_r}$ uitrekenen, want $\overline{K_l}^{-1}$ bestaat omdat $\det(\overline{K_l}) \neq 0$.

Nu heeft Eve dus sleutels $\overline{K_l}$ en $\overline{K_r}$ gevonden die elke plaintext P naar exact dezelfde ciphertext C sturen als de oorspronkelijke sleutels K_l en K_r doen.

Voorbeeld 2.13. We nemen opnieuw $K_l = \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix}$ en $K_r = \begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix}$, net zoals in Voorbeeld 2.8. Ook nu kent Eve deze sleutels niet. (Merk op dat beide sleutels nog altijd inverteerbaar zijn.) Voor een plaintext attack vult Eve eerst de plaintext $P^I = I$ in in $K_l \cdot P \cdot K_r$:

$$C^I \equiv \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix} \equiv \begin{pmatrix} 24 & 17 \\ 21 & 7 \end{pmatrix}$$

Oftewel:

$$K_l \cdot K_r \equiv M \equiv \begin{pmatrix} 24 & 17 \\ 21 & 7 \end{pmatrix}$$

$$(K_l \cdot K_r)^{-1} \equiv M^{-1} \equiv \begin{pmatrix} 24 & 17 \\ 21 & 7 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 15 & 5 \\ 13 & 10 \end{pmatrix}$$

Daarna kiest Eve achtereenvolgens de matrices

$$P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \; P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

en vult deze in in $K_l \cdot P \cdot K_r$. Het blijkt dat ze respectievelijk de volgende matrices (modulo 29) als ciphertext terugkrijgt:

$$C^\alpha \equiv \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix} \equiv \begin{pmatrix} 20 & 5 \\ 23 & 13 \end{pmatrix}$$
$$C^\beta \equiv \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 27 & 14 \\ 7 & 21 \end{pmatrix} \equiv \begin{pmatrix} 17 & 22 \\ 21 & 5 \end{pmatrix}$$

Nu kan Eve Q^α en Q^β berekenen (mod 29):

$$Q^\alpha \equiv C^\alpha \cdot (K_l \cdot K_r)^{-1} \equiv \begin{pmatrix} 20 & 5 \\ 23 & 13 \end{pmatrix} \cdot \begin{pmatrix} 15 & 5 \\ 13 & 10 \end{pmatrix} \equiv \begin{pmatrix} 17 & 5 \\ 21 & 13 \end{pmatrix}$$

$$Q^\beta \equiv C^\beta \cdot (K_l \cdot K_r)^{-1} \equiv \begin{pmatrix} 17 & 22 \\ 21 & 5 \end{pmatrix} \cdot \begin{pmatrix} 15 & 5 \\ 13 & 10 \end{pmatrix} \equiv \begin{pmatrix} 19 & 15 \\ 3 & 10 \end{pmatrix}$$

We hadden beredeneerd dat zou moeten gelden $Q \cdot K_l \equiv K_l \cdot P \pmod{29}$. Dus:

$$Q^\alpha \cdot K_l \equiv K_l \cdot P^\alpha \implies \begin{pmatrix} 17 & 5 \\ 21 & 13 \end{pmatrix} \cdot \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \equiv \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} l_1 & 0 \\ l_3 & 0 \end{pmatrix}$$

$$Q^\beta \cdot K_l \equiv K_l \cdot P^\beta \implies \begin{pmatrix} 19 & 15 \\ 3 & 10 \end{pmatrix} \cdot \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \equiv \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & l_1 \\ 0 & l_3 \end{pmatrix}$$

$\implies$

$$\begin{aligned} q_1^\alpha l_1 + q_2^\alpha l_3 &\equiv 17\ l_1 + 5\ l_3 \equiv l_1 && (11)\\ q_1^\alpha l_2 + q_2^\alpha l_4 &\equiv 17\ l_2 + 5\ l_4 \equiv 0 && (12)\\ q_3^\alpha l_1 + q_4^\alpha l_3 &\equiv 21\ l_1 + 13\ l_3 \equiv l_3 && (13)\\ q_3^\alpha l_2 + q_4^\alpha l_4 &\equiv 21\ l_2 + 13\ l_4 \equiv 0 && (14) \end{aligned}$$

$$\begin{aligned} q_1^\beta l_1 + q_2^\beta l_3 &\equiv 19\ l_1 + 15\ l_3 \equiv 0 && (15)\\ q_1^\beta l_2 + q_2^\beta l_4 &\equiv 19\ l_2 + 15\ l_4 \equiv l_1 && (16)\\ q_3^\beta l_1 + q_4^\beta l_3 &\equiv 3\ l_1 + 10\ l_3 \equiv 0 && (17)\\ q_3^\beta l_2 + q_4^\beta l_4 &\equiv 3\ l_2 + 10\ l_4 \equiv l_3 && (18) \end{aligned}$$

$\overset{(15)}{\implies}$

$$l_1 = \frac{-15}{19}\ l_3 \equiv -15 \cdot 26\ l_3 \equiv 16\ l_3 \quad (19)$$

$\overset{(12)}{\implies}$

$$l_2 = \frac{-5}{17}\ l_4 \equiv -5 \cdot 12\ l_4 \equiv 27\ l_4 \quad (20)$$

$\overset{(16)+(20)}{\implies}$

$$\begin{aligned} l_1 \equiv 19\ l_2 + 15\ l_4 \equiv 19 \cdot 27\ l_4 + 15\ l_4 &\equiv 6\ l_4 && (21)\\ &\equiv 26\ l_2 && (22) \end{aligned}$$

$\implies$

$$K_l \equiv \begin{pmatrix} l_1 & \frac{1}{26}\ l_1 \\ \frac{1}{16}\ l_1 & \frac{1}{6}\ l_1 \end{pmatrix} \equiv \begin{pmatrix} l_1 & 19\ l_1 \\ 20\ l_1 & 5\ l_1 \end{pmatrix}$$

Eve kiest nu $l_1 = \overline{l_1} = 1$ (hoewel elke waarde uit $\{1, 2, ..., 28\}$ volstaat), waardoor haar $\overline{K_l}$ nu wordt:

$$\overline{K_l} = \begin{pmatrix} 1 & 19 \\ 20 & 5 \end{pmatrix}$$

Uit Stelling 2.12 hebben we kunnen afleiden dat

$$\overline{K_l} \cdot \overline{K_r} \equiv K_l \cdot K_r \equiv M \equiv \begin{pmatrix} 24 & 17 \\ 21 & 7 \end{pmatrix}$$

Uit $\overline{K_l} = \begin{pmatrix} 1 & 19 \\ 20 & 5 \end{pmatrix}$ en $\overline{K_l} \cdot \overline{K_r} \equiv \begin{pmatrix} 24 & 17 \\ 21 & 7 \end{pmatrix} \pmod{29}$ kunnen we $\overline{K_r}$ nu bepalen:

$$\overline{K_r} \equiv \overline{K_l}^{-1} \cdot \overline{K_l} \cdot \overline{K_r} \equiv \begin{pmatrix} 1 & 19 \\ 20 & 5 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 24 & 17 \\ 21 & 7 \end{pmatrix} \equiv \begin{pmatrix} 20 & 5 \\ 17 & 22 \end{pmatrix}$$

En dus vindt Eve de sleutels

$$\overline{K_l} = \begin{pmatrix} 1 & 19 \\ 20 & 5 \end{pmatrix}, \quad \overline{K_r} = \begin{pmatrix} 20 & 5 \\ 17 & 22 \end{pmatrix}$$

zodat ze elke ciphertext kan kraken. ◁

Opmerking 2.14. Als Eve in het vorige voorbeeld $l_1 = 19$ had gekozen, dan zou ze de oorspronkelijke linkersleutel $K_l = \begin{pmatrix} 19 & 13 \\ 3 & 8 \end{pmatrix}$ hebben gevonden. Met behulp van $K_l \cdot K_r$ zou ze vervolgens ook de door Alice en Bob gekozen rechtersleutel K_r hebben kunnen bepalen. Met de sleutels die Eve nu gevonden heeft zal ze echter ook wel tevreden zijn. ◁

Ook via Methode 2 kan Eve in het vervolg dus bij elke ciphertext de plaintext achterhalen.

Samenvatting 2.15. Methode 2 kunnen we als volgt samenvatten:

- Eve berekent eerst het product $K_l \cdot K_r$ door te kijken wat de ciphertext is van $P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Noem deze ciphertext M.
- Dan voert ze opnieuw een plaintext attack uit door te bepalen wat de ciphertext is van de boodschap $P^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ respectievelijk $P^\beta = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Noem deze ciphertext C^α respectievelijk C^β.
- Nu berekent zij $Q^\alpha \equiv C^\alpha \cdot M^{-1}$ en $Q^\beta \equiv C^\beta \cdot M^{-1} \pmod{29}$.
- Eve stelt nu acht vergelijkingen op die zij verkrijgt uit de matrixvergelijkingen

$$Q^\alpha \cdot K_l \equiv K_l \cdot P^\alpha \quad \text{en} \quad Q^\beta \cdot K_l \equiv K_l \cdot P^\beta$$

- Met behulp van deze acht vergelijkingen drukt zij l_2, l_3, l_4 uit in termen van l_1. Nu kan zij K_l uitdrukken in l_1'tjes. Kies $l_1 = \overline{l_1} = 1$, dan is $\overline{K_l}$ bekend.
- Bereken nu $\overline{K_r}$ uit $\overline{K_l}$ en $M \equiv K_l \cdot K_r \equiv \overline{K_l} \cdot \overline{K_r} \pmod{29}$. Nu heeft Eve een combinatie $\overline{K_l}, \overline{K_r}$ van sleutels die exact dezelfde werking op een zekere plaintext heeft als de oorspronkelijke sleutels K_l en K_r.

◁

Opmerking 2.16. In plaats van de twee matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ en $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ hadden we ook twee willekeurige onafhankelijke matrices P^α en P^β voor de plaintext attack kunnen nemen. Immers, als P^α en P^β onafhankelijk zijn dan zijn $P^\alpha \cdot K \equiv C^\alpha$ en $P^\beta \cdot K \equiv C^\beta \pmod{29}$ onafhankelijk en dus zijn $C^\alpha \cdot M^{-1} \equiv Q^\alpha$ en $C^\beta \cdot M^{-1} \equiv Q^\beta \pmod{29}$ onafhankelijk. Hierdoor krijgen we voldoende onafhankelijke vergelijkingen om l_2, l_3, l_4 uit te drukken in termen van l_1. De resterende stappen in Methode 2 blijven ongewijzigd. ◁

Opmerking 2.17. Voor Methode 2 is het van belang dat Eve weet wat $K_l \cdot K_r \pmod{29}$ is. We hebben gezien dat dit alleen mogelijk is wanneer zij een plaintext attack kan uitvoeren met de plaintext $P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Een dergelijke plaintext attack noemen we een *chosen-plaintext*

attack. (Na deze chosen-plaintext attack met de eenheidsmatrix voert Eve nog een plaintext attack uit met de twee matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ en $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, of, zoals in de vorige opmerking te lezen was, twee willekeurige onafhankelijke matrices. In dit laatste geval noemen we deze aanval, zoals eerder vermeld, een known-plaintext attack.) $\triangleleft$

3 Generalisatie van de sleutellengte

3.1 $n = 2$ dan alles oké?

Het doel van deze scriptie is om te kijken of het mogelijk en, belangrijker, of het zinvol is om de Hill-cipher aan te passen van de vorm $P \cdot M$ naar $K_l \cdot P \cdot K_r$. In paragraaf 2.1 hebben we onszelf daarom twee vragen gesteld, namelijk:

- Is het vermenigvuldigen van links met een matrix K_l en het vermenigvuldigen van rechts met een matrix K_r wezenlijk anders dan de (aangepaste) Hill-cipher (i.e. het enkel vermenigvuldigen van rechts met een matrix K) of komt dit op hetzelfde neer?
- (*Indien de nieuwe Hill-cipher inderdaad anders is dan de originele Hill-cipher.*) Zijn de sleutels K_l en K_r bij het links respectievelijk rechts vermenigvuldigen van de plaintext makkelijk te achterhalen, zoals ook de sleutel bij de Hill-cipher makkelijk te achterhalen is?

In het vorige hoofdstuk hebben we een antwoord op deze vragen gegeven voor sleutellengte $n = 2$, dat wil zeggen: K_l en K_r zijn 2×2 matrices. Nu zullen we de vragen in een breder perspectief proberen te beantwoorden: zijn de antwoorden op de vragen voor een algemene sleutellengte n hetzelfde als voor het geval $n = 2$? Met andere woorden: is het vermenigvuldigen met K_l en K_r voor alle n wezenlijk anders dan enkel en alleen vermenigvuldigen met M en kunnen we voor elke n een methode ontwikkelen om de sleutels K_l en K_r te achterhalen? We gaan het zien in dit hoofdstuk...

3.2 Niet-uniciteit van M

Om een antwoord te geven op de eerste vraag moeten we onderzoeken of we voor alle boodschappen P het product $K_l \cdot P \cdot K_r$ zouden kunnen herschrijven als $P \cdot M$ voor een zekere vaste matrix M. Oftewel: gaat Stelling 2.4 op voor alle sleutellengtes n?

Als we even rustig nadenken, dan komen we tot de conclusie dat deze vraag er helemaal niet meer toe doet. We hebben namelijk voor het geval $n = 2$ aangetoond dat onze nieuwe Hill-cipher wezenlijk anders is dan de oorspronkelijke Hill-cipher. De reden waarom we hoopten dat M door de keuze van K_l en K_r vast zou liggen – en dus het doel van Stelling 2.4 – was dat het idee om de oude Hill-cipher aan te passen in ieder geval geen kinderachtig idee zou zijn. En dat dit inderdaad niet zo is bleek uit Stelling 2.4.

Uiteraard geeft dit nog geen antwoord op de vraag of M vastligt voor alle mogelijke sleutellengtes, maar als we, net zoals voor $n = 2$, ook een methode kunnen ontwikkelen om de nieuwe Hill-cipher voor alle n te kraken, dan is de vraag die in dit paragraafje centraal staat niet meer relevant. Immers, als M wél voor alle P vastligt door de keuze van K_l en K_r, dan zijn we niet blij, want dan hebben we een orginele Hill-cipher en die is eenvoudig te kraken. Maar als M niet vastligt en er bestaat voor alle sleutellengtes een methode om de sleutels te achterhalen, dan is Eve ook degene die het laatst lacht. Als we de methodes om de sleutels K_l en K_r voor het geval $n = 2$ te kraken kunnen generaliseren, dan is het dus hoe dan ook huilen met de pet op voor Alice en Bob...

3.3 Sleutels van willekeurige lengte kraken

We zullen nu gaan kijken of we Methode 1 en 2 kunnen veralgemeniseren naar alle mogelijke sleutellengtes n. Hierbij is het van belang dat Lemma 2.5 nog steeds opgaat. Vandaar dat we ons hier eerst op zullen richten.

Lemma 3.1. *Voor alle sleutels K_l en K_r van lengte n kunnen er sleutels $\overline{K_l}$ en $\overline{K_r}$ van dezelfde lengte worden gevonden, zodanig dat $\overline{K_l} \neq K_l$ en $\overline{K_r} \neq K_r$ en $K_l \cdot P \cdot K_r \equiv \overline{K_l} \cdot P \cdot \overline{K_r}$ modulo 29 voor alle P.*
Bewijs: We rekenen modulo 29, dus elk getal $x \in \{1, 2, 3, ..., 28\}$ heeft een inverse modulo 29. Daarom volgt, mits $l_{1,1} \neq 0$:

$$K_l \cdot P \cdot K_r \equiv \begin{pmatrix} l_{1,1} & l_{1,2} & \cdots & l_{1,n} \\ l_{2,1} & l_{2,2} & \cdots & l_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1} & l_{n,2} & \cdots & l_{n,n} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,n} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1} & r_{n,2} & \cdots & r_{n,n} \end{pmatrix}$$

$$\equiv l_{1,1} \begin{pmatrix} 1 & \frac{l_{1,2}}{l_{1,1}} & \cdots & \frac{l_{1,n}}{l_{1,1}} \\ \frac{l_{2,1}}{l_{1,1}} & \frac{l_{2,2}}{l_{1,1}} & \cdots & \frac{l_{2,n}}{l_{1,1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{l_{n,1}}{l_{1,1}} & \frac{l_{n,2}}{l_{1,1}} & \cdots & \frac{l_{n,n}}{l_{1,1}} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,n} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1} & r_{n,2} & \cdots & r_{n,n} \end{pmatrix}$$

$$\equiv \begin{pmatrix} 1 & \frac{l_{1,2}}{l_{1,1}} & \cdots & \frac{l_{1,n}}{l_{1,1}} \\ \frac{l_{2,1}}{l_{1,1}} & \frac{l_{2,2}}{l_{1,1}} & \cdots & \frac{l_{2,n}}{l_{1,1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{l_{n,1}}{l_{1,1}} & \frac{l_{n,2}}{l_{1,1}} & \cdots & \frac{l_{n,n}}{l_{1,1}} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} l_{1,1}r_{1,1} & l_{1,1}r_{1,2} & \cdots & l_{1,1}r_{1,n} \\ l_{1,1}r_{2,1} & l_{1,1}r_{2,2} & \cdots & l_{1,1}r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ l_{1,1}r_{n,1} & l_{1,1}r_{n,2} & \cdots & l_{1,1}r_{n,n} \end{pmatrix}$$

$$\equiv \begin{pmatrix} \overline{l_{1,1}} & \overline{l_{1,2}} & \cdots & \overline{l_{1,n}} \\ \overline{l_{2,1}} & \overline{l_{2,2}} & \cdots & \overline{l_{2,n}} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{l_{n,1}} & \overline{l_{n,2}} & \cdots & \overline{l_{n,n}} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} \overline{r_{1,1}} & \overline{r_{1,2}} & \cdots & \overline{r_{1,n}} \\ \overline{r_{2,1}} & \overline{r_{2,2}} & \cdots & \overline{r_{2,n}} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{r_{n,1}} & \overline{r_{n,2}} & \cdots & \overline{r_{n,n}} \end{pmatrix}$$

$$\equiv \overline{K_l} \cdot P \cdot \overline{K_r}$$

Als $l_{1,1} = 0$ dan kunnen we hetzelfde trucje uithalen met $l_{1,2}$. Als die ook weer gelijk is aan 0 dan pakken we $l_{1,3}$, etc. (Merk op dat er een $k \in \{1, 2, ..., n\}$ bestaat zodanig dat $l_{1,k} \neq 0$, want $\det(K_l) = 0$.) ◁

Gevolg 3.2. *Laat n de lengte van de sleutels van een (geüpdatete) Hill-cipher zijn. Dan zijn er minstens 28 verschillende combinaties K_l, K_r zodanig dat $K_{l_u} \cdot P \cdot K_{r_u} \equiv K_{l_v} \cdot P \cdot K_{r_v}$ modulo 29 voor alle $u, v \in \{1, 2, ..., 28\}$ en voor alle P.*
Bewijs: Als $l_{1,1_u} \neq 0$ dan kunnen we K_{l_u} met een constante $d \in \{1, 2, 3, ..., 28\}$ en K_{r_u} met $\frac{1}{d}$

(mod 29) vermenigvuldigen, zodat $l_{1,1_u}$ de waarden $\{1, 2, ..., 28\}$ kan aannemen:

$$K_{l_u} \cdot P \cdot K_{r_u} \equiv \begin{pmatrix} l_{1,1_u} & l_{1,2_u} & \cdots & l_{1,n_u} \\ l_{2,1_u} & l_{2,2_u} & \cdots & l_{2,n_u} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1_u} & l_{n,2_u} & \cdots & l_{n,n_u} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} r_{1,1_u} & r_{1,2_u} & \cdots & r_{1,n_u} \\ r_{2,1_u} & r_{2,2_u} & \cdots & r_{2,n_u} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1_u} & r_{n,2_u} & \cdots & r_{n,n_u} \end{pmatrix}$$

$$\equiv d \cdot \frac{1}{d} \begin{pmatrix} l_{1,1_u} & l_{1,2_u} & \cdots & l_{1,n_u} \\ l_{2,1_u} & l_{2,2_u} & \cdots & l_{2,n_u} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1_u} & l_{n,2_u} & \cdots & l_{n,n_u} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} r_{1,1_u} & r_{1,2_u} & \cdots & r_{1,n_u} \\ r_{2,1_u} & r_{2,2_u} & \cdots & r_{2,n_u} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1_u} & r_{n,2_u} & \cdots & r_{n,n_u} \end{pmatrix}$$

$$\equiv \begin{pmatrix} d\ l_{1,1_u} & d\ l_{1,2_u} & \cdots & d\ l_{1,n_u} \\ d\ l_{2,1_u} & d\ l_{2,2_u} & \cdots & d\ l_{2,n_u} \\ \vdots & \vdots & \ddots & \vdots \\ d\ l_{n,1_u} & d\ l_{n,2_u} & \cdots & d\ l_{n,n_u} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} \frac{1}{d}\ r_{1,1_u} & \frac{1}{d}\ r_{1,2_u} & \cdots & \frac{1}{d}\ r_{1,n_u} \\ \frac{1}{d}\ r_{2,1_u} & \frac{1}{d}\ r_{2,2_u} & \cdots & \frac{1}{d}\ r_{2,n_u} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{d}\ r_{n,1_u} & \frac{1}{d}\ r_{n,2_u} & \cdots & \frac{1}{d}\ r_{n,n_u} \end{pmatrix}$$

$$\equiv \begin{pmatrix} l_{1,1_v} & l_{1,2_v} & \cdots & l_{1,n_v} \\ l_{2,1_v} & l_{2,2_v} & \cdots & l_{2,n_v} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1_v} & l_{n,2_v} & \cdots & l_{n,n_v} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} r_{1,1_v} & r_{1,2_v} & \cdots & r_{1,n_v} \\ r_{2,1_v} & r_{2,2_v} & \cdots & r_{2,n_v} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1_v} & r_{n,2_v} & \cdots & r_{n,n_v} \end{pmatrix}$$

$$\equiv K_{l_v} \cdot P \cdot K_{r_v}$$

Als $l_{1,1_u} = 0$ dan geldt hetzelfde argument voor $l_{1,2_u}$ (of $l_{1,3_u}$, etc.).
Zo krijgen we 28 verschillende combinaties K_l, K_r. Elke combinatie verstuurt een willekeurige plaintext naar een en dezelfde ciphertext. ◁

We zien dat Lemma 2.5 en Gevolg 2.6 blijven gelden voor elke mogelijke sleutellengte. Dit biedt perspectief voor Methode 1 om te slagen.

3.3.1 Methode 1

In het geval $n = 2$ kan Eve met behulp van vier bewust gekozen boodschappen een plaintext attack uitvoeren. Eens kijken of zij op soortgelijke wijze dezelfde schade kan aanrichten bij sleutels van willekeurige lengte. Hiertoe voeren we eerst een notatie in:

$$P^{i,j} = \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix}$$

waarbij voor elke positie $p_{k,l}$ in matrix $P^{i,j}$ geldt: $p_{k,l} = \begin{cases} 1 & \text{als } k = i, l = j \\ 0 & \text{als anders} \end{cases}$.

Nu bereidt Eve een plaintext attack voor. Zij kiest alle mogelijke matrices $P^{i,j}$ (dit zijn er

n^2). (Het is eenvoudig na te gaan dat deze matrices onafhankelijk zijn.) Als we een plaintext P in de snoepautomaat gooien, dan voldoet de ciphertext aan de onderstaande gelijkheden:

$$K_l \cdot P \cdot K_r \equiv \begin{pmatrix} l_{1,1} & l_{1,2} & \cdots & l_{1,n} \\ l_{2,1} & l_{2,2} & \cdots & l_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1} & l_{n,2} & \cdots & l_{n,n} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,n} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1} & r_{n,2} & \cdots & r_{n,n} \end{pmatrix}$$

$$\equiv \begin{pmatrix} \sum_{i=1}^{n} l_{1,i}p_{i,1} & \sum_{i=1}^{n} l_{1,i}p_{i,2} & \cdots & \sum_{i=1}^{n} l_{1,i}p_{i,n} \\ \sum_{i=1}^{n} l_{2,i}p_{i,1} & \sum_{i=1}^{n} l_{2,i}p_{i,2} & \cdots & \sum_{i=1}^{n} l_{2,i}p_{i,n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^{n} l_{n,i}p_{i,1} & \sum_{i=1}^{n} l_{n,i}p_{i,2} & \cdots & \sum_{i=1}^{n} l_{n,i}p_{i,n} \end{pmatrix} \begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,n} \\ r_{2,1} & r_{2,2} & \cdots & r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1} & r_{n,2} & \cdots & r_{n,n} \end{pmatrix}$$

$$\equiv \begin{pmatrix} \sum_{j=1}^{n}\sum_{i=1}^{n} l_{1,i}p_{i,j}r_{j,1} & \sum_{j=1}^{n}\sum_{i=1}^{n} l_{1,i}p_{i,i}r_{j,2} & \cdots & \sum_{j=1}^{n}\sum_{i=1}^{n} l_{1,i}p_{i,j}r_{j,n} \\ \sum_{j=1}^{n}\sum_{i=1}^{n} l_{2,i}p_{i,j}r_{j,1} & \sum_{j=1}^{n}\sum_{i=1}^{n} l_{2,i}p_{i,j}r_{j,2} & \cdots & \sum_{j=1}^{n}\sum_{i=1}^{n} l_{2,i}p_{i,j}r_{j,n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{j=1}^{n}\sum_{i=1}^{n} l_{n,i}p_{i,j}r_{j,1} & \sum_{j=1}^{n}\sum_{i=1}^{n} l_{n,i}p_{i,j}r_{j,2} & \cdots & \sum_{j=1}^{n}\sum_{i=1}^{n} l_{n,i}p_{i,j}r_{j,n} \end{pmatrix}$$

$$\equiv \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & c_{n,2} & \cdots & c_{n,n} \end{pmatrix}$$

$$\equiv C$$

Als Eve nu de eerder genoemde n^2 matrices als plaintext invult, dan krijg zij n^2 stelsels van ieder n^2 vergelijkingen, oftewel n^4 vergelijkingen (mod 29):

$$P^{1,1} \implies \begin{cases} l_{1,1}r_{1,1} \equiv c_{1,1}^{1,1} & l_{1,1}r_{1,2} \equiv c_{1,2}^{1,1} & \cdots & l_{1,1}r_{1,n} \equiv c_{1,n}^{1,1} \\ l_{2,1}r_{1,1} \equiv c_{2,1}^{1,1} & l_{2,1}r_{1,2} \equiv c_{2,2}^{1,1} & \cdots & l_{2,1}r_{1,n} \equiv c_{2,n}^{1,1} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1}r_{1,1} \equiv c_{n,1}^{1,1} & l_{n,1}r_{1,2} \equiv c_{n,2}^{1,1} & \cdots & l_{n,1}r_{1,n} \equiv c_{n,n}^{1,1} \end{cases}$$

$$P^{1,2} \implies \begin{cases} l_{1,1}r_{2,1} \equiv c_{1,1}^{1,2} & l_{1,1}r_{2,2} \equiv c_{1,2}^{1,2} & \cdots & l_{1,1}r_{2,n} \equiv c_{1,n}^{1,2} \\ l_{2,1}r_{2,1} \equiv c_{2,1}^{1,2} & l_{2,1}r_{2,2} \equiv c_{2,2}^{1,2} & \cdots & l_{2,1}r_{2,n} \equiv c_{2,n}^{1,2} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1}r_{2,1} \equiv c_{n,1}^{1,2} & l_{n,1}r_{2,2} \equiv c_{n,2}^{1,2} & \cdots & l_{n,1}r_{2,n} \equiv c_{n,n}^{1,2} \end{cases}$$

$$\vdots$$

$$P^{1,n} \quad \Longrightarrow \quad \begin{cases} l_{1,1}r_{n,1} \equiv c_{1,1}^{1,n} & l_{1,1}r_{n,2} \equiv c_{1,2}^{1,n} & \cdots & l_{1,1}r_{n,n} \equiv c_{1,n}^{1,n} \\ l_{2,1}r_{n,1} \equiv c_{2,1}^{1,n} & l_{2,1}r_{n,2} \equiv c_{2,2}^{1,n} & \cdots & l_{2,1}r_{n,n} \equiv c_{2,n}^{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1}r_{n,1} \equiv c_{n,1}^{1,n} & l_{n,1}r_{n,2} \equiv c_{n,2}^{1,n} & \cdots & l_{n,1}r_{n,n} \equiv c_{n,n}^{1,n} \end{cases}$$

$$P^{2,1} \quad \Longrightarrow \quad \begin{cases} l_{1,2}r_{1,1} \equiv c_{1,1}^{2,1} & l_{1,2}r_{1,2} \equiv c_{1,2}^{2,1} & \cdots & l_{1,2}r_{1,n} \equiv c_{1,n}^{2,1} \\ l_{2,2}r_{1,1} \equiv c_{2,1}^{2,1} & l_{2,2}r_{1,2} \equiv c_{2,2}^{2,1} & \cdots & l_{2,2}r_{1,n} \equiv c_{2,n}^{2,1} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,2}r_{1,1} \equiv c_{n,1}^{2,1} & l_{n,2}r_{1,2} \equiv c_{n,2}^{2,1} & \cdots & l_{n,2}r_{1,n} \equiv c_{n,n}^{2,1} \end{cases}$$

$$\vdots$$

$$P^{n,n} \quad \Longrightarrow \quad \begin{cases} l_{1,n}r_{n,1} \equiv c_{1,1}^{n,n} & l_{1,n}r_{n,2} \equiv c_{1,2}^{n,n} & \cdots & l_{1,n}r_{n,n} \equiv c_{1,n}^{n,n} \\ l_{2,n}r_{n,1} \equiv c_{2,1}^{n,n} & l_{2,n}r_{n,2} \equiv c_{2,2}^{n,n} & \cdots & l_{2,n}r_{n,n} \equiv c_{2,n}^{n,n} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,n}r_{n,1} \equiv c_{n,1}^{n,n} & l_{n,n}r_{n,2} \equiv c_{n,2}^{n,n} & \cdots & l_{n,n}r_{n,n} \equiv c_{n,n}^{n,n} \end{cases}$$

Hierbij stelt $c_{k,l}^{i,j}$ het getal voor dat op positie k, l staat in de ciphertextmatrix behorende bij de plaintext $P^{i,j}$.

Uit Lemma 3.1 volgt dat we deze n^4 vergelijkingen ook als volgt kunnen opvatten (mod 29):

$$P^{1,1} \quad \Longrightarrow \quad \begin{cases} \overline{l_{1,1}}\ \overline{r_{1,1}} \equiv c_{1,1}^{1,1} & \overline{l_{1,1}}\ \overline{r_{1,2}} \equiv c_{1,2}^{1,1} & \cdots & \overline{l_{1,1}}\ \overline{r_{1,n}} \equiv c_{1,n}^{1,1} \\ \overline{l_{2,1}}\ \overline{r_{1,1}} \equiv c_{2,1}^{1,1} & \overline{l_{2,1}}\ \overline{r_{1,2}} \equiv c_{2,2}^{1,1} & \cdots & \overline{l_{2,1}}\ \overline{r_{1,n}} \equiv c_{2,n}^{1,1} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{l_{n,1}}\ \overline{r_{1,1}} \equiv c_{n,1}^{1,1} & \overline{l_{n,1}}\ \overline{r_{1,2}} \equiv c_{n,2}^{1,1} & \cdots & \overline{l_{n,1}}\ \overline{r_{1,n}} \equiv c_{n,n}^{1,1} \end{cases}$$

$$P^{1,2} \quad \Longrightarrow \quad \begin{cases} \overline{l_{1,1}}\ \overline{r_{2,1}} \equiv c_{1,1}^{1,2} & \overline{l_{1,1}}\ \overline{r_{2,2}} \equiv c_{1,2}^{1,2} & \cdots & \overline{l_{1,1}}\ \overline{r_{2,n}} \equiv c_{1,n}^{1,2} \\ \overline{l_{2,1}}\ \overline{r_{2,1}} \equiv c_{2,1}^{1,2} & \overline{l_{2,1}}\ \overline{r_{2,2}} \equiv c_{2,2}^{1,2} & \cdots & \overline{l_{2,1}}\ \overline{r_{2,n}} \equiv c_{2,n}^{1,2} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{l_{n,1}}\ \overline{r_{2,1}} \equiv c_{n,1}^{1,2} & \overline{l_{n,1}}\ \overline{r_{2,2}} \equiv c_{n,2}^{1,2} & \cdots & \overline{l_{n,1}}\ \overline{r_{2,n}} \equiv c_{n,n}^{1,2} \end{cases}$$

$$\vdots$$

$$P^{1,n} \quad \Longrightarrow \quad \begin{cases} \overline{l_{1,1}}\ \overline{r_{n,1}} \equiv c_{1,1}^{1,n} & \overline{l_{1,1}}\ \overline{r_{n,2}} \equiv c_{1,2}^{1,n} & \cdots & \overline{l_{1,1}}\ \overline{r_{n,n}} \equiv c_{1,n}^{1,n} \\ \overline{l_{2,1}}\ \overline{r_{n,1}} \equiv c_{2,1}^{1,n} & \overline{l_{2,1}}\ \overline{r_{n,2}} \equiv c_{2,2}^{1,n} & \cdots & \overline{l_{2,1}}\ \overline{r_{n,n}} \equiv c_{2,n}^{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{l_{n,1}}\ \overline{r_{n,1}} \equiv c_{n,1}^{1,n} & \overline{l_{n,1}}\ \overline{r_{n,2}} \equiv c_{n,2}^{1,n} & \cdots & \overline{l_{n,1}}\ \overline{r_{n,n}} \equiv c_{n,n}^{1,n} \end{cases}$$

$$P^{2,1} \quad \Longrightarrow \quad \begin{cases} \overline{l_{1,2}}\ \overline{r_{1,1}} \equiv c_{1,1}^{2,1} & \overline{l_{1,2}}\ \overline{r_{1,2}} \equiv c_{1,2}^{2,1} & \cdots & \overline{l_{1,2}}\ \overline{r_{1,n}} \equiv c_{1,n}^{2,1} \\ \overline{l_{2,2}}\ \overline{r_{1,1}} \equiv c_{2,1}^{2,1} & \overline{l_{2,2}}\ \overline{r_{1,2}} \equiv c_{2,2}^{2,1} & \cdots & \overline{l_{2,2}}\ \overline{r_{1,n}} \equiv c_{2,n}^{2,1} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{l_{n,2}}\ \overline{r_{1,1}} \equiv c_{n,1}^{2,1} & \overline{l_{n,2}}\ \overline{r_{1,2}} \equiv c_{n,2}^{2,1} & \cdots & \overline{l_{n,2}}\ \overline{r_{1,n}} \equiv c_{n,n}^{2,1} \end{cases}$$

$$\vdots$$

$$P^{n,n} \quad \Longrightarrow \quad \begin{cases} \overline{l_{1,n}}\ \overline{r_{n,1}} \equiv c_{1,1}^{n,n} & \overline{l_{1,n}}\ \overline{r_{n,2}} \equiv c_{1,2}^{n,n} & \cdots & \overline{l_{1,n}}\ \overline{r_{n,n}} \equiv c_{1,n}^{n,n} \\ \overline{l_{2,n}}\ \overline{r_{n,1}} \equiv c_{2,1}^{n,n} & \overline{l_{2,n}}\ \overline{r_{n,2}} \equiv c_{2,2}^{n,n} & \cdots & \overline{l_{2,n}}\ \overline{r_{n,n}} \equiv c_{2,n}^{n,n} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{l_{n,n}}\ \overline{r_{n,1}} \equiv c_{n,1}^{n,n} & \overline{l_{n,n}}\ \overline{r_{n,2}} \equiv c_{n,2}^{n,n} & \cdots & \overline{l_{n,n}}\ \overline{r_{n,n}} \equiv c_{n,n}^{n,n} \end{cases}$$

Nu kiest Eve $\overline{l_{1,1}} = 1$. Met behulp van de vergelijkingen behorende bij de n boodschappen $P^{1,k}$, met $1 \leq k \leq n$, kan zij nu $\overline{r_{i,j}}$ bepalen voor alle $i, j \in \{1, 2, ..., n\}$. (Merk op dat zij hiervoor n^2 vergelijkingen moet oplossen.) Hierna kan Eve, gebruikmakende van de vergelijkingen die horen bij de n matrices $P^{k,1}$, met $1 \leq k \leq n$, $\overline{l_{i,j}}$ berekenen voor alle $i, j \in \{1, 2, ..., n\}$. (Dit zijn $n^2 - 1$ stuks, want $\overline{l_{1,1}}$ kende ze al.) In totaal moet Eve dus $2n^2 - 1$ vergelijkingen oplossen, nadat ze $\overline{l_{1,1}}$ gekozen heeft. Dit is ook logisch, want er zijn opgeteld precies $2n^2$ l- en r'tjes.

Eve heeft haar doel bereikt: zij heeft nu sleutels $\overline{K_l}$ en $\overline{K_r}$ van lengte n gevonden die elke plaintext P aan dezelfde ciphertext koppelen als dat de sleutels K_l en K_r van Alice en Bob gedaan zouden hebben.

Samenvatting 3.3. De generalisatie van Methode 1 kunnen we als volgt samenvatten:

- Eve voert een plaintext attack uit: ze neemt de n^2 onafhankelijke matrices $(1 \leq i, j \leq n)$

$$P^{i,j} = \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix}$$

  waarbij voor elke positie $p_{k,l}$ in matrix $P^{i,j}$ geldt: $p_{k,l} = \begin{cases} 1 & \text{als } k = i, l = j \\ 0 & \text{als anders} \end{cases}$ en kijkt wat de bijbehorende gecodeerde boodschappen zijn; hieruit verkrijgt zij n^4 vergelijkingen.
- Zij kiest $\overline{l_{1,1}} = 1$, waardoor de overige $2n^2 - 1$ $\overline{l_{i,j}}$, $\overline{r_{i,j}}$ vast komen te liggen. Deze kan Eve uitrekenen, zodat zij $\overline{K_l}$ en $\overline{K_r}$ kan bepalen.
- Nu kan Eve bij elke ciphertext C de bijbehorende plaintext $P \equiv \overline{K_l}^{-1} \cdot C \cdot \overline{K_r}^{-1} \pmod{29}$ uitrekenen.

$\lhd$

Opmerking 3.4. Net zoals we hebben opgemerkt bij Methode 1 voor sleutellengte 2 geldt ook nu weer dat Eve niet per se een plaintext attack hoeft uit te voeren met matrices die bestaan uit louter nullen en een een. Elke known-plaintext attack met n^2 onafhankelijke matrices voldoet (zie Opmerking 2.10 voor de redenering waarom dit zo is), hoewel Eve niet vrolijk zal worden van de hieruit verkregen vergelijkingen. $\lhd$

3.3.2 Methode 2

Net zoals in het geval $n = 2$ willen we de nieuwe Hill-cipher $K_l \cdot P \cdot K_r$ herschrijven naar $Q \cdot M$ voor een vaste M. Neem ook nu weer (mod 29)

$$\begin{aligned} Q &\equiv K_l \cdot P \cdot K_l^{-1} \\ M &\equiv K_l \cdot K_r \end{aligned}$$

zodat de plaintext P een basistransformatie heeft ondergaan (Q is geconjugeerd met P) en M een sleutel van de oorspronkelijke Hill-cipher is.

Als Eve $P = I_n$ neemt, dan volgt:

$$K_l \cdot P \cdot K_r \equiv K_l \cdot I_n \cdot K_r \equiv K_l \cdot K_r \equiv M \pmod{29}$$

Oftewel: door de eenheidsmatrix als plaintext te nemen krijgt zij matrix M als ciphertext.

Uit $Q \equiv K_l \cdot P \cdot K_l^{-1} \pmod{29}$ volgt dat moet gelden $Q \cdot K_l \equiv K_l \cdot P \pmod{29}$. In vol ornaat (mod 29):

$$\begin{aligned} Q \cdot K_l &\equiv \begin{pmatrix} q_{1,1} & q_{1,2} & \cdots & q_{1,n} \\ q_{2,1} & q_{2,2} & \cdots & q_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ q_{n,1} & q_{n,2} & \cdots & q_{n,n} \end{pmatrix} \begin{pmatrix} l_{1,1} & l_{1,2} & \cdots & l_{1,n} \\ l_{2,1} & l_{2,2} & \cdots & l_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1} & l_{n,2} & \cdots & l_{n,n} \end{pmatrix} \\ &\equiv \begin{pmatrix} \sum_{i=1}^n q_{1,i}l_{i,1} & \sum_{i=1}^n q_{1,i}l_{i,2} & \cdots & \sum_{i=1}^n q_{1,i}l_{i,n} \\ \sum_{i=1}^n q_{2,i}l_{i,1} & \sum_{i=1}^n q_{2,i}l_{i,2} & \cdots & \sum_{i=1}^n q_{2,i}l_{i,n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n q_{n,i}l_{i,1} & \sum_{i=1}^n q_{n,i}l_{i,2} & \cdots & \sum_{i=1}^n q_{n,i}l_{i,n} \end{pmatrix} \\ &\equiv \begin{pmatrix} \sum_{i=1}^n l_{1,i}p_{i,1} & \sum_{i=1}^n l_{1,i}p_{i,2} & \cdots & \sum_{i=1}^n l_{1,i}p_{i,n} \\ \sum_{i=1}^n l_{2,i}p_{i,1} & \sum_{i=1}^n l_{2,i}p_{i,2} & \cdots & \sum_{i=1}^n l_{2,i}p_{i,n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n l_{n,i}p_{i,1} & \sum_{i=1}^n l_{n,i}p_{i,2} & \cdots & \sum_{i=1}^n l_{n,i}p_{i,n} \end{pmatrix} \\ &\equiv \begin{pmatrix} l_{1,1} & l_{1,2} & \cdots & l_{1,n} \\ l_{2,1} & l_{2,2} & \cdots & l_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n,1} & l_{n,2} & \cdots & l_{n,n} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{pmatrix} \\ &\equiv K_l \cdot P \end{aligned}$$

We zien dat uit bovenstaande vergelijkingen n^2 gelijkheden voortvloeien:

$$\sum_{i=1}^n q_{u,i}l_{i,v} \equiv \sum_{i=1}^n l_{u,i}p_{i,v} \pmod{29} \text{ voor alle } u, v \in \{1, 2, ..., n\}$$

Vervolgens voert Eve weer een plaintext attack uit. Ditmaal neemt zij de n matrices $P^{1,k}$, met $1 \leq k \leq n$.[3] Voor elke matrix $P^{1,k}$ vindt Eve n^2 vergelijkingen, waarvan zij er n kan gebruiken om $l_{i,k}$ voor alle $i \in \{1, 2, ..., n\}$ en voor vaste k uit te drukken in termen van $l_{1,1}$. (Mocht dit niet meteen glashelder zijn voor de lezer dan volgt zo direct een voorbeeld waaruit zal blijken dat we geen onzin lopen te verkopen.) Door $P^{1,k}$ voor elke $k \in \{1, 2, ..., n\}$ langs te lopen kan Eve alle $l_{i,j}$, $i, j \in \{1, 2, ..., n\}$ in termen van $l_{1,1}$ uitdrukken, zeg

$$K_l = \begin{pmatrix} l_{1,1} & \mu_{1,2}l_{1,1} & \cdots & \mu_{1,n}l_{1,1} \\ \mu_{2,1}l_{1,1} & \mu_{2,2}l_{1,1} & \cdots & \mu_{2,n}l_{1,1} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{n,1}l_{1,1} & \mu_{n,2}l_{1,1} & \cdots & \mu_{n,n}l_{1,1} \end{pmatrix}$$

met $\mu_{i,j} \in \{0, 1, 2, ..., 28\}$ voor alle $i, j \in \{1, 2, ..., n\}$.

Uit Lemma 3.1 volgt dat er sleutels $\overline{K_l}, \overline{K_r}$ bestaan die dezelfde werking hebben als K_l, K_r. Voor elke keuze van $l_{1,1}$ in bovenstaande matrix is K_l is dus een goede sleutel. Kies nu $l_{1,1} = 1$ en laat $\overline{K_l}$ de zo ontstane linkersleutel zijn. Eve kent nu zowel $\overline{K_l}$ als $K_l \cdot K_r$. We weten dat $K_l \cdot P \cdot K_r \equiv \overline{K_l} \cdot P \cdot \overline{K_r} \pmod{29}$ voor alle boodschappen P, dus in het bijzonder voor $P = I_n$. Hieruit volgt dat $K_l \cdot K_r \equiv \overline{K_l} \cdot \overline{K_r} \pmod{29}$. En dus kan Eve uit $\overline{K_l}$ en $(K_l \cdot K_r \equiv)\ \overline{K_l} \cdot \overline{K_r} \pmod{29}$ ook $\overline{K_r}$ bepalen, want $\overline{K_l}$ is inverteerbaar.

En voilà, Eve kan de boodschap van elke ciphertext achterhalen.

Voorbeeld 3.5. Hier volgt nog een klein voorbeeld om de pessimisten onder ons te overtuigen dat het nemen van de matrices $P^{1,k}$ voor alle $k \in \{1, 2, ..., n\}$ voldoende is om alle $l_{i,j}$ uit te drukken in termen van $l_{1,1}$.
Stel de sleutellengte is 3. Dan krijgen we (mod 29):

$$\begin{aligned} Q \cdot K_l &\equiv \begin{pmatrix} q_{1,1} & q_{1,2} & q_{1,3} \\ q_{2,1} & q_{2,2} & q_{2,3} \\ q_{3,1} & q_{3,2} & q_{3,3} \end{pmatrix} \begin{pmatrix} l_{1,1} & l_{1,2} & l_{1,3} \\ l_{2,1} & l_{2,2} & l_{2,3} \\ l_{3,1} & l_{3,2} & l_{3,3} \end{pmatrix} \\ &\equiv \begin{pmatrix} l_{1,1} & l_{1,2} & l_{1,3} \\ l_{2,1} & l_{2,2} & l_{2,3} \\ l_{3,1} & l_{3,2} & l_{3,3} \end{pmatrix} \begin{pmatrix} p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,1} & p_{3,2} & p_{3,3} \end{pmatrix} \\ &\equiv K_l \cdot P \end{aligned}$$

[3] Hierbij is $P^{1,k}$ nog altijd de matrix die bijna volledig is gevuld met nullen; alleen op positie $1, k$ staat een 1; zie Methode 1.

Hieruit rollen de volgende vergelijkingen modulo 29:

$$P^{1,1} \implies \begin{cases} q_{1,1}l_{1,1} + q_{1,2}l_{2,1} + q_{1,3}l_{3,1} \equiv l_{1,1} \\ q_{1,1}l_{1,2} + q_{1,2}l_{2,2} + q_{1,3}l_{3,2} \equiv 0 \\ q_{1,1}l_{1,3} + q_{1,2}l_{2,3} + q_{1,3}l_{3,3} \equiv 0 \\ \\ q_{2,1}l_{1,1} + q_{2,2}l_{2,1} + q_{2,3}l_{3,1} \equiv l_{2,1} \\ q_{2,1}l_{1,2} + q_{2,2}l_{2,2} + q_{2,3}l_{3,2} \equiv 0 \\ q_{2,1}l_{1,3} + q_{2,2}l_{2,3} + q_{2,3}l_{3,3} \equiv 0 \\ \\ q_{3,1}l_{1,1} + q_{3,2}l_{2,1} + q_{3,3}l_{3,1} \equiv l_{3,1} \\ q_{3,1}l_{1,2} + q_{3,2}l_{2,2} + q_{3,3}l_{3,2} \equiv 0 \\ q_{3,1}l_{1,3} + q_{3,2}l_{2,3} + q_{3,3}l_{3,3} \equiv 0 \end{cases}$$

$$P^{1,2} \implies \begin{cases} q_{1,1}l_{1,1} + q_{1,2}l_{2,1} + q_{1,3}l_{3,1} \equiv 0 \\ q_{1,1}l_{1,2} + q_{1,2}l_{2,2} + q_{1,3}l_{3,2} \equiv l_{1,1} \\ q_{1,1}l_{1,3} + q_{1,2}l_{2,3} + q_{1,3}l_{3,3} \equiv 0 \\ \\ q_{2,1}l_{1,1} + q_{2,2}l_{2,1} + q_{2,3}l_{3,1} \equiv 0 \\ q_{2,1}l_{1,2} + q_{2,2}l_{2,2} + q_{2,3}l_{3,2} \equiv l_{2,1} \\ q_{2,1}l_{1,3} + q_{2,2}l_{2,3} + q_{2,3}l_{3,3} \equiv 0 \\ \\ q_{3,1}l_{1,1} + q_{3,2}l_{2,1} + q_{3,3}l_{3,1} \equiv 0 \\ q_{3,1}l_{1,2} + q_{3,2}l_{2,2} + q_{3,3}l_{3,2} \equiv l_{3,1} \\ q_{3,1}l_{1,3} + q_{3,2}l_{2,3} + q_{3,3}l_{3,3} \equiv 0 \end{cases}$$

$$P^{1,3} \implies \begin{cases} q_{1,1}l_{1,1} + q_{1,2}l_{2,1} + q_{1,3}l_{3,1} \equiv 0 \\ q_{1,1}l_{1,2} + q_{1,2}l_{2,2} + q_{1,3}l_{3,2} \equiv 0 \\ q_{1,1}l_{1,3} + q_{1,2}l_{2,3} + q_{1,3}l_{3,3} \equiv l_{1,1} \\ \\ q_{2,1}l_{1,1} + q_{2,2}l_{2,1} + q_{2,3}l_{3,1} \equiv 0 \\ q_{2,1}l_{1,2} + q_{2,2}l_{2,2} + q_{2,3}l_{3,2} \equiv 0 \\ q_{2,1}l_{1,3} + q_{2,2}l_{2,3} + q_{2,3}l_{3,3} \equiv l_{2,1} \\ \\ q_{3,1}l_{1,1} + q_{3,2}l_{2,1} + q_{3,3}l_{3,1} \equiv 0 \\ q_{3,1}l_{1,2} + q_{3,2}l_{2,2} + q_{3,3}l_{3,2} \equiv 0 \\ q_{3,1}l_{1,3} + q_{3,2}l_{2,3} + q_{3,3}l_{3,3} \equiv l_{3,1} \end{cases}$$

Met behulp van de eerste, de vierde en de zevende vergelijking bij $P^{1,1}$ kunnen we $l_{2,1}$ en $l_{3,1}$ uitdrukken in termen van $l_{1,1}$ (alle $q_{i,j}$ met $1 \leq i, j \leq 3$ zijn namelijk bekend). Vervolgens drukken we $l_{1,2}$, $l_{2,2}$ en $l_{3,2}$ uit in $l_{1,1}$ met behulp van de tweede, vijfde en achtste vergelijking bij $P^{1,2}$. En tot slot brengen de derde, zesde en negende vergelijking bij $P^{1,3}$ ons helemaal in Hosannastemming door $l_{1,3}$, $l_{2,3}$ en $l_{3,3}$ in termen van $l_{1,1}$ uit te laten drukken. Op deze manier hebben we een linkersleutel in elkaar geknutseld die enkel en alleen afhangt van de keuze voor $l_{1,1}$ (die we 1 zullen laten zijn). Hoe de sleutel(s) verder te kraken is (zijn), daar weet Eve wel raad mee.

De lezer kan inzien dat dit voor alle sleutellengtes n goed gaat. $\triangleleft$

Samenvatting 3.6. De generalisatie van Methode 2 kunnen we als volgt samenvatten:

- Eve berekent eerst het product $K_l \cdot K_r$ door te kijken wat de ciphertext is van $P = I_n$, waar n de sleutellengte is (een chosen-plaintext attack dus). Noem deze ciphertext M.
- Dan voert ze een plaintext attack uit door te bepalen wat de ciphertext is van de boodschappen $P^{1,k}$ voor alle $k \in \{1, 2, ..., n\}$. Noem deze gecodeerde boodschappen $C^{1,k}$ voor alle $k \in \{1, 2, ..., n\}$.
- Nu berekent zij $Q^{1,k} \equiv C^{1,k} \cdot M^{-1} \pmod{29}$ voor alle $k \in \{1, 2, ..., n\}$.
- Voor elke $k \in \{1, 2, ..., n\}$ stelt Eve nu n^2 vergelijkingen op die zij verkrijgt uit de matrixvergelijking $Q^{1,k} \cdot K_l \equiv K_l \cdot P^{1,k} \pmod{29}$.
- Met behulp van deze vergelijkingen drukt zij $l_{i,j}$ voor alle $i, j \in \{1, 2, ..., n\}$ uit in termen van $l_{1,1}$. Nu kan zij K_l uitdrukken in $l_{1,1}$'tjes. Kies $l_{1,1} = \overline{l_{1,1}} = 1$, dan is $\overline{K_l}$ bekend.
- Bereken nu $\overline{K_r}$ uit $\overline{K_l}$ en $M \equiv K_l \cdot K_r \equiv \overline{K_l} \cdot \overline{K_r} \pmod{29}$. Nu heeft Eve een combinatie $\overline{K_l}, \overline{K_r}$ van sleutels die exact dezelfde werking op een zekere plaintext heeft als de oorspronkelijke sleutels K_l en K_r.

$\triangleleft$

Opmerking 3.7. Ook voor een willekeurige sleutellengte n hoeft Eve niet per se gebruik te maken van de door ons opgedragen boodschappen. Hoewel zij verplicht is om een chosen-plaintext attack uit te voeren met $P = I_n$ (omdat zij per se $K_l \cdot K_r$ moet achterhalen), is het geoorloofd om vervolgens een known-plaintext attack uit te voeren met n onafhankelijke matrices, in plaats van de hierboven voorgeschreven matrices $P^{1,k}$. (De redenering waarom dit zo is is analoog aan die in Opmerking 2.16.) $\triangleleft$

4 Conclusies

De door Lester Hill bedachte Hill-cipher eenvoudig is te kraken met behulp van een plaintext attack. In deze scriptie hebben we een balletje opgegooid om de oorspronkelijke Hill-cipher $P \cdot K \equiv C$ aan te passen naar de vorm $K_l \cdot P \cdot K_r \equiv C$, waarbij P een plaintext en C een ciphertext is en waarbij K_l en K_r encryptiesleutels zijn, erop hopende dat de Hill-cipher hierdoor veilig(er) werd. Helaas bleek dit niet het geval te zijn. We hebben een tweetal methoden gegeven – eerst voor sleutellengte 2 en vervolgens uitgebreid naar een willekeurige sleutellengte n – om deze vernieuwde Hill-cipher te kraken.

Methode 1 behoeft een known-plaintext attack van n^2 onafhankelijke matrices; voor Methode 2 is een chosen-plaintext attack met $P = I_n$ nodig (waarbij I_n de eenheidsmatrix is met sleutellengte n), gevolgd door een known-plaintext attack met n onafhankelijke matrices. Voor Methode 2 zijn dus minder matrices nodig, maar het rekenwerk dat vervolgens staat te wachten bij de ontstane vergelijkingen is vele malen groter. Het is dus maar net waar Eve haar voorkeur aan geeft.

Om een lang verhaal kort te maken: het is voor Alice en Bob niet verstandig om (een variant op) de Hill-cipher als cryptosysteem te kiezen.

Referenties

[1] Trappe, Wade; Washington, Lawrence C.: *Introduction to Cryptography with Coding Theory.* Pearson Higher Education, Second Edition, 2005, pp. 34-38.

[2] Hill, Lester S.: *Cryptography in an Algebraic Alphabet.* The American Mathematical Monthly, Vol. 36, No. 6 (Jun.-Jul., 1929), pp. 306-312, http://w08.middlebury.edu/INTD1065A/Lectures/Hill%20Cipher%20Folder/Hill1.pdf