Linear Ciphers

Klaus Pommerening
Fachbereich Physik, Mathematik, Informatik
der Johannes-Gutenberg-Universität
Saarstraße 21
D-55099 Mainz

January 16, 2000—English version July 28, 2014—last change
January 19, 2021

In 1929 the mathematician Lester Hill proposed the use of matrices for encryption. He published his idea in the American Mathematical Monthly. This cryptographic application of linear algebra piqued the curiosity of mathematicians. But its obvious weaknesses soon became evident, so it never found a serious application. The true importance of the method relied on the fact that it was the first systematic use of algebraic methods in cryptology. And by the way its cryptanalysis made clear how dangerous linearity in encryption functions is.

> Jack Levine later mentioned that he used this kind of cipher already in 1924 for a contribution to a youth magazine when he was a high-school student.

In this section we use the appendix on the Euclidean algorithm.

1 Matrices over Rings

Let R be a ring (commutative with 1). The "multiplicative group" of R is the group of invertible elements

$$R^\times = \{a \in R \mid ab = 1 \text{ for some } b \in R\} = \{a \in R \mid a \text{ divides } 1\}.$$

In the same way the (non-commutative) R-algebra $M_{qq}(R)$ of $q \times q$-matrices over R has a group of invertible elements ("general linear group")

$$GL_q(R) = \{A \in M_{qq}(R) \mid AB = \mathbf{1}_q \text{ for some } B \in M_{qq}(R)\}.$$

The determinant defines a multiplicative map

$$\operatorname{Det}\colon M_{qq}(R) \longrightarrow R,$$

and

$$A \in GL_q(R) \Longrightarrow AB = \mathbf{1}_q \text{ for some } B \Longrightarrow \operatorname{Det} A \cdot \operatorname{Det} B = \operatorname{Det} \mathbf{1}_q = 1$$

$$\Longrightarrow \operatorname{Det} A \in R^\times.$$

The converse implication is also true. For a proof we consider the adjoint matrix $\tilde{A} = (\tilde{a}_{ij})$ where

$$\tilde{a}_{ij} = A_{ji} = \operatorname{Det} \begin{pmatrix} a_{11} & \dots & a_{1,i-1} & a_{1,i+1} & \dots & a_{1q} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{j-1,1} & \dots & a_{j-1,i-1} & a_{j-1,i+1} & \dots & a_{j-1,q} \\ a_{j+1,1} & \dots & a_{j+1,i-1} & a_{j+1,i+1} & \dots & a_{j+1,q} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{q1} & \dots & a_{q,i-1} & a_{q,i+1} & \dots & a_{qq} \end{pmatrix}$$

Using this we can prove:

Proposition 1 *For $A \in M_{qq}(R)$ the following holds:*
(i) $A\tilde{A} = \operatorname{Det} A \cdot \mathbf{1}_q$.
(ii) $A \in GL_q(R) \Longleftrightarrow \operatorname{Det} A \in R^\times$*; if this is true, then*

$$A^{-1} = \frac{1}{\operatorname{Det} A}\tilde{A}.$$

Proof. (i) is the expansion rule for determinants.
(ii) immediately follows from (i). $\diamond$

In particular Det induces a group homomorphism $GL_q(R) \longrightarrow R^\times$.

Example For $R = \mathbb{Z}/n\mathbb{Z}$ the statement (ii) of Proposition 1 can be rewritten as:

$$A \in M_{qq}(\mathbb{Z}) \text{ is invertible } \mod n \iff \operatorname{Det} A \text{ is coprime with } n.$$

Remarks

1. The expenses for calculating the inverse matrix A^{-1} are, if statement (ii) is naively evaluated:
   - one $q \times q$-determinant with $q!$ summands, each with q factors,
   - q^2 determinants of size $(q-1) \times (q-1)$.

   This is extremely inefficient—it is exponential in q.
2. Using GAUSSian elimination the expenses drop to $\mathrm{O}(q^3)$. But this is not quite true: Exact calculation produces rational numbers with *huge* numerators and denominators that require additional resources.

There is a modification of the elimination algorithm that uses only integers and is much more efficient, see the next section. However also this procedure produces large intermediate results.

An alternative algorithm uses the Chinese Remainder Theorem: Each ring homomorphism $\varphi\colon R \longrightarrow R'$ induces a homomorphism of R-algebras

$$\varphi_q\colon M_{qq}(R) \longrightarrow M_{qq}(R')$$

by componentwise evaluation. If $A \in M_{qq}$ is invertible, then

$$\varphi_q(A)\varphi_q(A^{-1}) = \varphi_q(AA^{-1}) = \varphi_q(\mathbf{1}_q) = \mathbf{1}_q.$$

Hence also $\varphi_q(A)$ is invertible. Furthermore $\operatorname{Det}\varphi_q(A) = \varphi(\operatorname{Det} A)$, so we have a commutative diagram

$$\begin{array}{ccc} M_{qq}(R) & \xrightarrow{\varphi_q} & M_{qq}(R') \\ {\scriptstyle\operatorname{Det}}\downarrow & & \downarrow{\scriptstyle\operatorname{Det}} \\ R & \xrightarrow[\varphi]{} & R' \end{array}$$

Applying this to $R = \mathbb{Z}$ we use the residue class homomorphisms $\mathbb{Z} \longrightarrow \mathbb{F}_p$ (p prime) for sufficiently many primes p such that the product of these primes is $> \operatorname{Det} A$. Then we calculate

- $\operatorname{Det} A \bmod p$ in all the fields $\mathbb{F}_p$ (avoiding huge numbers, since all intermediate results may be represented as numbers between 0 and $p-1$),
- $\operatorname{Det} A \in \mathbb{Z}$ using the Chinese Remainder Theorem.

2 Elimination over the Integers

How to solve systems of linear equations over the ring $\mathbb{Z}$ of integers? How to calculate determinants efficiently? How to find an inverse matrix? Like in linear algebra over fields also in the more general situation over rings the *triangularization* of matrices is crucial for finding efficient algorithms.

For a sufficiently general framework we consider three classes of rings (commutative, with 1, without zero divisors):

- **Factorial rings** (or UFD domains): All elements have a decomposition into primes, in particular any two elements have a greatest common divisor gcd (in general not unique).
- **Principal ideal domains:** Each ideal is a principal ideal. Principal ideal domains are factorial, and the gcd of any two elements is a linear combination of these two.
- **Euclidean rings:** They have a division with remainder. Euclidean rings are principal ideal domains. The gcd of two elements as well as its linear represenation can be efficiently calculated by the extended Euclidean algorithm.

The set of invertible matrices with determinant 1 over a ring is called the "special linear group" $SL_n(R) \subseteq GL_n(R)$. It is the kernel of the determinant homomorphism on $GL_n(R)$.

Lemma 1 *Let R be a principal ideal domain, $a_1, \ldots, a_n \in R$, and d a $\gcd(a_1, \ldots, a_n)$. Then there is an invertible matrix $U \in SL_n(R)$ such that*

$$U \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Proof. Since the case $n = 1$ is trivial we may assume $n \geq 2$.

If all $a_i = 0$, then the assertion is trivial. Otherwise we may assume without restriction that $a_1 \neq 0$ (after a permutation that is merged into U as permutation matrix—if necessary replace a 1 by -1 to make the determinant $= 1$).

Let $d_2 := \gcd(a_1, a_2)$ (*any* gcd because in general this is not unique). Then $d_2 \neq 0$ and $d_2 = c_1 a_1 + c_2 a_2$ is a linear combination. From this we get the equation

$$\begin{pmatrix} c_1 & c_2 \\ -\frac{a_2}{d_2} & \frac{a_1}{d_2} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} c_1 a_1 + c_2 a_2 \\ -\frac{a_2 a_1}{d_2} + \frac{a_1 a_2}{d_2} \end{pmatrix} = \begin{pmatrix} d_2 \\ 0 \end{pmatrix}$$

where the matrix of coefficients

$$C = \begin{pmatrix} c_1 & c_2 \\ -\frac{a_2}{d_2} & \frac{a_1}{d_2} \end{pmatrix} \quad \text{has } \operatorname{Det} C = \frac{c_1 a_1}{d_2} + \frac{c_2 a_2}{d_2} = 1$$

and therefore is invertible.

We proceed be induction: Assume for the general step that for some $i \geq 2$

$$U' \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d' \\ 0 \\ \vdots \\ 0 \\ a_i \\ \vdots \\ a_n \end{pmatrix} \qquad \text{where } a_i \neq 0$$

Then as before we change two coordinates:

$$\begin{pmatrix} d' \\ a_i \end{pmatrix} \rightsquigarrow \begin{pmatrix} d'' \\ 0 \end{pmatrix}.$$

In this way we successively build the matrix U. $\diamond$

Remark The inverse of the matrix C in the proof is

$$C^{-1} = \begin{pmatrix} \frac{a_1}{d_2} & -c_2 \\ \frac{a_2}{d_2} & c_1 \end{pmatrix}$$

From this formula we see that U and U^{-1} together can be calculated by at most $n-1$ executions of the Euclidean algorithm, plus $n-1$ multiplications of $n \times n$-matrices plus at most $n-1$ multiplications of permutation matrices.

With the help of this lemma we can triangularise matrices. (A more refined analysis would lead to the HERMITEan normal form.)

Theorem 1 (i) *Let R be a principal ideal domain, and $A \in M_{pq}(R)$. Then there exists an invertible matrix $U \in SL_p(R)$ such that $H = UA$ has the form*

$$\begin{pmatrix} * & \dots & * \\ & \ddots & \vdots \\ & & * \\ 0 & & \end{pmatrix} \quad \text{für } p \geq q, \qquad \begin{pmatrix} * & \dots & \dots & * \\ & \ddots & \dots & \\ 0 & & * & \end{pmatrix} \quad \text{für } p < q.$$

(ii) *If R is Euclidean, then U and U^{-1} together can be calculated by at most $\frac{p(p-1)}{2}$ executions of the extended Euclidean algorithm.*

Special case Let $A \in M_{pp}(R)$ be a square matrix, and determine $H = UA$ as in the Theorem. Then

$$\operatorname{Det} A = \operatorname{Det} H = h_{11} \cdots h_{pp}.$$

If A is invertible, then $A^{-1} = (U^{-1}H)^{-1} = H^{-1}U$. The calculation of the inverse H^{-1} of the triangular matrix H is easy. Thus calculation of determinant and inverse are reduced to triangularisation.

Proof. We prove this by describing an algorithm. Let $r := \min\{p, q\}$. Initialize the algorithm by

$$H := A, \quad U := \mathbf{1}_p, \quad V := \mathbf{1}_p.$$

Then loop over $j = 1, \ldots r$. The relations $UA = H$, $UV = \mathbf{1}_p$ are loop invariants.

- Assume that at the beginning of the j-th step H has the form:

$$\begin{pmatrix} * & & & & \\ & \ddots & & & * \\ & & * & & \\ & & & h_{jj} & \\ & 0 & & \vdots & \\ & & & h_{pj} & \end{pmatrix}$$

If $h_{jj} = \ldots = h_{pj} = 0$ we finish step j. Otherwise we use the lemma and find a matrix $U' \in SL_{p-j+1}(R)$ together with its inverse $(U')^{-1}$ such that

$$U' \begin{pmatrix} h_{jj} \\ \ldots \\ h_{pj} \end{pmatrix} = \begin{pmatrix} d_j \\ 0 \\ \ldots \\ 0 \end{pmatrix}$$

We have $\left(\begin{smallmatrix} \mathbf{1} & 0 \\ 0 & U' \end{smallmatrix}\right) \in SL_p(R)$. At the end of the loop we replace

$$U := \begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} U, \quad H := \begin{pmatrix} \mathbf{1} & 0 \\ 0 & U' \end{pmatrix} H, \quad V := V \begin{pmatrix} \mathbf{1} & 0 \\ 0 & (U')^{-1} \end{pmatrix}.$$

After finishing the last loop U and H have the desired form. $\diamond$

Summarizing the expenses we have to add $\frac{p(p-1)}{2}$ matrix multiplications and the same number of multiplications by permutation matrices. However the total expenses are not yet covered because bounds for the intermediate results are yet missing. More exact considerations give expenses of the order $\mathrm{O}(m^2n^5)$ where m is an upper bound for the number of digits of the entries of A and $n = \max(p, q)$. For further optimizations of this bound search the literature on algebraic algorithms.

Elimination in Residue Class Rings

Now how to invert a matrix $A \in GL_q(\mathbb{Z}/n\mathbb{Z})$? First interpret A as an integer matrix and determine $U \in SL_q(\mathbb{Z})$ such that $H = UA$ is an integer upper triangular matrix as in Theorem 1. Reduction $\bmod n$ conserves the equation $H = UA$ as well as $A^{-1} = H^{-1}U$. Since $A \bmod n$ is invertible all diagonal elements of H are invertible $\bmod n$.

3 The Linear Cipher

Description

The **alphabet** is $\Sigma = \mathbb{Z}/n\mathbb{Z}$ with the structure as a finite ring.

The **keyspace** is $K = GL_l(\mathbb{Z}/n\mathbb{Z})$, the multiplicative group of invertible matrices. Section 4 estimates the size of the keyspace.

We **encrypt** blockwise taking blocks of length l: For $k \in GL_l(\mathbb{Z}/n\mathbb{Z})$ and $(a_1, \ldots, a_l) \in (\mathbb{Z}/n\mathbb{Z})^l$ set

$$\begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix} = f_k(a_1, \ldots, a_l) = k \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix}$$

or elementwise

$$c_i = \sum_{j=1}^{l} k_{ij} a_j \quad \text{for } i = 1, \ldots, l.$$

We **decrypt** with the inverse matrix:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix} = k^{-1} \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix}.$$

Related Ciphers

Special case: Taking k as permutation matrix P_σ for a permutation $\sigma \in \mathcal{S}_l$ the encryption function f_k is the block transposition defined by σ.

Generalization: The affine cipher. Choose as key a pair

$$(k, b) \in GL_l(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^l.$$

Encrypt by the formula

$$c = ka + b.$$

Choosing the unit matrix for k (as special case) gives the Bellaso cipher with key b.

Remark The original cipher proposed by Hill first permuted the alphabet before applying the linear map. The correspondence between the letters and the numbers $0, \ldots, 25$ is treated as part of the key.

Example

As an illustration we take a "toy example" of unreasonable small dimension $l = 2$ and

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

Then $\operatorname{Det} k = 77 - 24 = 53 \equiv 1 \bmod 26$ and

$$k^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

The table

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

gives the correspondence between letters and numbers.

Now the plaintext `Herr` $= (7, 4, 17, 17)$ is encrypted as

$$\begin{aligned} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} &= \begin{pmatrix} 77 + 32 \\ 21 + 28 \end{pmatrix} = \begin{pmatrix} 109 \\ 49 \end{pmatrix} = \begin{pmatrix} 5 \\ 23 \end{pmatrix}, \\ \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 17 \\ 17 \end{pmatrix} &= \begin{pmatrix} 187 + 136 \\ 51 + 119 \end{pmatrix} = \begin{pmatrix} 323 \\ 170 \end{pmatrix} = \begin{pmatrix} 11 \\ 14 \end{pmatrix}. \end{aligned}$$

Thus $f_k(\texttt{Herr}) = (5, 23, 11, 14) = \texttt{FXLO}$.

We verify this by decrypting:

$$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} = \begin{pmatrix} 35 + 414 & 77 + 252 \\ 115 + 253 & 253 + 154 \end{pmatrix} = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}.$$

Assessment

\+ The linear cipher is stronger than block transposition and Bellaso cipher.

\+ The frequency distribution of the ciphertext letters is nearly uniform. An attack with ciphertext only doesn't find useful clues.

\− The linear cipher is extremely vulnerable for an attack with known plaintext, see Section 5.

4 The Number of Invertible Matrices over a Residue Class Ring

We want as clearly as possible to get an idea how large the number

$$\nu_{ln} := \#GL_l(\mathbb{Z}/n\mathbb{Z})$$

of invertible $l \times l$ matrices over the residue class ring $\mathbb{Z}/n\mathbb{Z}$ is.

In the special case $l = 1$ the number ν_{1n} simply counts the invertible elements of $\mathbb{Z}/n\mathbb{Z}$ and is given as the value $\varphi(n)$ of the EULER φ-function.

In the general case we easily find a trivial *upper bound* for ν_{ln}:

$$\nu_{ln} \leq \#M_{ll}(\mathbb{Z}/n\mathbb{Z}) = n^{l^2}.$$

To find a *lower bound* we note that (over any ring R) matrices of the form

$$\begin{pmatrix} 1 & & \\ & \ddots & \\ * & & 1 \end{pmatrix} \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_l \end{pmatrix} \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$$

are always invertible if $d_1, \ldots, d_l \in R^\times$. This gives an injective map

$$R^{\frac{l(l-1)}{2}} \times (R^\times)^l \times R^{\frac{l(l-1)}{2}} \longrightarrow GL_l(R).$$

(Proof of injectivity: **Exercise.**) This gives the bound

$$\nu_{ln} \geq n^{\frac{l(l-1)}{2}} \cdot \varphi(n)^l \cdot n^{\frac{l(l-1)}{2}} = n^{l^2-l} \cdot \varphi(n)^l.$$

Taken together this yields:

Proposition 2

$$n^{l^2-l} \cdot \varphi(n)^l \leq \nu_{ln} \leq n^{l^2}.$$

Remarks

1. The idea of writing matrices as $A = VDW$ as above—where D is a diagonal matrix, V, a lower triangular matrix with only 1's in the diagonal, and W, an upper triangular matrix likewise with only 1's in the diagonal—gives an easy way of constructing invertible matrices without resorting to trial and error and calculating determinants. This method gives "almost all" invertible matrices—in the theory of algebraic groups this is the "big BRUHAT cell". Matrices of this type can be easily inverted by the formula $A^{-1} = W^{-1}D^{-1}V^{-1}$.

2. Two lower bounds for the φ-function that we cite without proofs yield handy bounds for ν_{ln}. The first of these bounds is

$$\varphi(n) > \frac{6}{\pi^2} \cdot \frac{n}{\ln n} \quad \text{for } n \geq 7.$$

   This yields

$$\nu_{ln} > n^{l^2-l} \cdot \left(\frac{6}{\pi^2} \cdot \frac{n}{\ln n} \right)^l = \frac{6^l}{\pi^{2l}} \cdot \frac{n^{l^2}}{(\ln n)^l} \quad \text{for } n \geq 7.$$

3. The other bound is

$$\varphi(n) > \frac{n}{2 \cdot \ln \ln n} \quad \text{for almost all } n.$$

   This yields

$$\nu_{ln} > \frac{1}{(2 \cdot \ln \ln n)^l} \cdot n^{l^2}$$

   or

$$\frac{1}{(2 \cdot \ln \ln n)^l} \quad < \quad \frac{\nu_{ln}}{n^{l^2}} \quad < \quad 1$$

   for almost all n.

Conclusion "Very many" to "almost all" matrices in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ are invertible. But also note that asymptotically the quotient ν_{ln}/n^{l^2} is not bounded away from 0.

Example For $n = 26$ we give a coarser but very simple version of the lower bound from Proposition 2: From $\varphi(26) = 12$ we get

$$\nu_{l,26} \geq 26^{l^2-l} 12^l > 16^{l^2-l} 8^l = 2^{4l^2-l}.$$

This gives the bounds $\nu_{2,26} > 2^{14}$, $\nu_{3,26} > 2^{33}$, $\nu_{4,26} > 2^{60}$, $\nu_{5,26} > 2^{95}$. We conclude that the linear cipher is secure from exhaustion at least for block size 5.

Finally we derive an exact formula for ν_{ln}.

Lemma 2 *Let $n = p$ prime. Then*

$$\nu_{lp} = p^{l^2} \cdot \rho_{lp} \quad \textit{where} \quad \rho_{lp} = \prod_{i=1}^{l} \left(1 - \frac{1}{p^i} \right).$$

In particular for fixed l the relative frequency of invertible matrices, ρ_{lp}, converges to 1 with increasing p.

Proof. We successively build an invertible matrix column by column and count the possibilities for each column. Since $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field the first column is an arbitrary vector $\neq 0$. This makes $p^l - 1$ choices.

Assume we have already chosen i columns. These must be linearly independent hence span a linear subspace of $\mathbb{F}_p^l$. This subspace consists of p^i elements. The $(i+1)$-th column then is an arbitrary vector outside of this subspace for which we have $p^l - p^i$ choices. Summing up this yields

$$\prod_{i=0}^{l-1}(p^l - p^i) = \prod_{i=0}^{l-1} p^l(1 - p^{i-l}) = p^{l^2} \prod_{j=1}^{l} \left(1 - \frac{1}{p^j}\right)$$

choices. ◇

Lemma 3 *Let $n = p^e$ with p prime and $e \geq 1$.*

(i) *Let $A \in M_{ll}(\mathbb{Z})$. Then $A \bmod n$ is invertible in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ if and only if $A \bmod p$ is invertible in $M_{ll}(\mathbb{F}_p)$.*

(ii) *The number of invertible matrices in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ is*

$$\nu_{ln} = n^{l^2} \cdot \rho_{lp}.$$

(iii) *The relative frequency of invertible matrices in $M_{ll}(\mathbb{Z}/p^e\mathbb{Z})$ is ρ_{lp}, independent of the exponent e.*

Proof. (i) Since $\gcd(p, \operatorname{Det} A) = 1 \iff \gcd(n, \operatorname{Det} A) = 1$, both statements are equivalent with $p \nmid \operatorname{Det} A$.

(ii) Without restriction we may assume that A has all its entries in $[0 \dots n-1]$. Then we write $A = pQ + R$ where all entries of R are in $[0 \dots p-1]$ and all entries of Q are in $[0 \dots p^{e-1} - 1]$. The matrix $A \bmod n$ is invertible if and only if $R \bmod p$ is invertible. For R we have ν_{lp} choices by Lemma 2, and for Q we have $p^{(e-1)l^2}$ choices. Taken together this proves the claim.

(iii) is a direct consequence of (ii). ◇

Lemma 4 *For m and n coprime $\nu_{l,mn} = \nu_{lm}\nu_{ln}$.*

Proof. The Chinese Remainder Theorem gives a ring isomorphism

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

and extends to an isomorphism of the (non-commutative) rings

$$M_{ll}(\mathbb{Z}/mn\mathbb{Z}) \longrightarrow M_{ll}(\mathbb{Z}/m\mathbb{Z}) \times M_{ll}(\mathbb{Z}/n\mathbb{Z}).$$

The assertion follows from the equality of the numbers of invertible elements. ◇

Induction immediately yields:

Theorem 2 *For $n \in \mathbb{N}$*

$$\nu_{ln} = n^{l^2} \cdot \prod_{\substack{p \text{ prime} \\ p|n}} \rho_{lp}.$$

In particular the relative frequency of invertible matrices $\rho_{ln} = \nu_{ln}/n^{l^2}$ is independent from the exponents of the prime factors of n. The explicit formula is

$$\rho_{ln} = \prod_{\substack{p \text{ prime} \\ p|n}} \rho_{lp} = \prod_{\substack{p \text{ prime} \\ p|n}} \prod_{i=1}^{l} \left(1 - \frac{1}{p^i}\right).$$

Example For $n = 26$ the explicit formula is

$$\nu_{l,26} = 26^{l^2} \cdot \prod_{i=1}^{l} \left(1 - \frac{1}{2^i}\right)\left(1 - \frac{1}{13^i}\right)$$

This evaluates as $\nu_{1,26} = 12$, $\nu_{2,26} = 157,248$, $\nu_{3,26} = 1,634,038,189,056 \approx 1.5 \cdot 2^{40}$. Comparing this value of $\nu_{3,26}$ with the lower bound 2^{33} from above shows how coarse this bound is. For $l = 4$ we even get $\nu_{4,26} \approx 1.3 \cdot 2^{73}$, almost secure from exhaustion.

Exercise Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... the increasing sequence of the primes. Let $n_r = p_1 \cdots p_r$ for $r \geq 1$. Show that for fixed l

$$\lim_{r \to \infty} \rho_{ln_r} = 0.$$

This means that the relative frequency of invertible matrices is decreasing for this sequence of moduli. *Hint*: Let ζ be the RIEMANN ζ-function. Which values has ζ at the natural numbers $i \geq 1$?

5 Cryptanalysis of the Linear Cipher

Block Length

The block length l leaves its trace as a divisor of the ciphertext length. If however the sender conceals the procedure by padding with meaningless text the cryptanalyst has no choice than to try all possible lengths by brute force.

Known Plaintext

Cryptanalyzing the linear cipher needs known plaintext—or some probable plaintext and a bit of trial and error to find the correct position. If the cryptanalyst knows the block length l and has l blocks of known plaintext she only has to solve a system of linear equations. This amounts to known plaintext of l^2 letters, corresponding to the length of the key. In a few degenerate cases she needs some additional known plaintext.

Let $(a_{11}, \ldots, a_{l1}), \ldots, (a_{1l}, \ldots, a_{ll})$ be the blocks of known plaintext, not necessarily contiguous, and $(c_{11}, \ldots, c_{l1}), \ldots, (c_{1l}, \ldots, c_{ll})$, the corresponding ciphertext blocks.

This yields the matrix equation

$$\begin{pmatrix} k_{11} & \ldots & k_{1l} \\ \vdots & \ddots & \vdots \\ k_{l1} & \ldots & k_{ll} \end{pmatrix} \begin{pmatrix} a_{11} & \ldots & a_{1l} \\ \vdots & \ddots & \vdots \\ a_{l1} & \ldots & a_{ll} \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1l} \\ \vdots & \ddots & \vdots \\ c_{l1} & \ldots & c_{ll} \end{pmatrix},$$

in short: $kA = C$ in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$. Note that the lowercase letter k also denotes an $l \times l$-matrix. In the lucky (but common) case where A is invertible we immediately solve for k and get the key

$$k = CA^{-1}.$$

Inverting a matrix is efficient by Section 2. Furthermore with high probability A is invertible, see Section 4. Otherwise the cryptanalyst needs some more plaintext. Instead of explicating the solution in detail we consider an example.

Example

Imagine the example of Section 3 is part of a longer text, and the plaintext `Herr` is known as well as its location. It consists of two blocks and defines the matrix

$$A = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}.$$

The determinant is $\operatorname{Det} A = 17 \cdot (7 \cdot 1 - 4 \cdot 1) = 17 \cdot 3 = 51 \equiv -1 \bmod 26$. The cryptanalyst has luck. She immediately calculates the inverse:

$$A^{-1} = \begin{pmatrix} 9 & 17 \\ 4 & 19 \end{pmatrix}.$$

From this she gets the key matrix:

$$k = \begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} \begin{pmatrix} 9 & 17 \\ 4 & 19 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

Solving the Affine Cipher

For solving the affine cipher $c = ka + b$ the cryptanalyst in general needs $l + 1$ blocks of known plaintext $a_0, \ldots, a_l$. By forming differences she gets

$$\begin{aligned} c_l - c_0 &= k \cdot (a_l - a_0), \\ &\ldots \\ c_l - c_{l-1} &= k \cdot (a_l - a_{l-1}). \end{aligned}$$

This reduces the cryptanalysis to that of the linear cipher with l known plaintext blocks.

Summary

Linearity makes a cipher extremely vulnerable for a known plaintext attack. The reason is that systems of linear equations are easily solved, at least over rings that allow practical calculations. (This however is a basic prerequisite for a ring to be useful for cryptography.)

In constructing secure ciphers on wants to prevent known plaintext attacks. Therefore one has to bring in nonlinearity: Solving algebraic equation of higher degree is much more complex. Hence the memento:

Known plaintext is adversary to linearity.

Exercise. Hill's proposal comprised a permutation of the alphabet before applying the linear map. That means executing a monoalphabetic substitution first. Explore the effect on cryptanalysis.