Transpositions

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

January16, 2000—English version July 25, 2014—last change August 25, 2014

All the cryptographic procedures that we considered up to now worked by replacing each plaintext letter by another one, letter per letter. In this chapter we follow a complementary approach: Don't change the letters but instead change their order. This approach also goes back to anitiquity.

1 Transpositions and Their Properties

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/Definition.html`

2 Examples

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/Examples.html`

Constructing a Turning Grille

Let $l \in \mathbb{N}$ be a natural number ≥ 2. Draw a $2l \times 2l$ square and divide it into four $l \times l$ squares.

1	$\ldots$	l		$\ldots$	1
$\vdots$		$\vdots$	$\vdots$		$\vdots$
	$\ldots$	l^2	l^2	$\ldots$	l
l	$\ldots$	l^2	l^2	$\ldots$	
$\vdots$		$\vdots$	$\vdots$		$\vdots$
1	$\ldots$		l	$\ldots$	1

In the first square (upper left) enumerate the positions consecutively from 1 to l^2, and transfer these numbers to the other three squares, rotating the scheme by 90° to the right in each step, as shown in the table above.

A key consists of a choice of one of the four $l \times l$ squares for each of the numbers $1, \ldots, l^2$. Then make a hole at the corresponding position in the corresponding square, for a total of l^2 holes.

Thus the size of the keyspace is 4^{l^2}. For small l this amounts to:

Parameter l:	3	4	5	6
# Keys:	2^{18}	2^{32}	2^{50}	2^{72}

For $l = 6$ or more the keyspace is sufficiently large. However this doesn't make the cipher secure.

3 Cryptanalysis of a Columnar Transposition (Example)

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/ColTrAnal.html`

4 Cryptanalytic Approaches

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/Approach.html`

Conditional Bigram Log-Weights

Let L be a language over the alphabet $\Sigma = (s_0, \ldots, s_{n-1})$ with letter probabilities p_i and bigram probabilities p_{ij} for the bigrams $s_i s_j$. Then the conditional bigram probabilities are given by

$$p_{j|i} = p_{ij}/p_i \quad \text{for } i, j = 0, \ldots, n-1.$$

The number $p_{j|i}$ is the probability that given the letter s_i as beginning of a bigram (an event that occurs with probability p_i) the second letter of the bigram is s_j. For convenience we set $p_{j|i} = 0$ if $p_i = 0$.

Then for a set of independent bigrams the probabilities multiply, and it's usual to consider the logarithms of the probabilties to get sums instead of products. Adding a constant to the sum amounts to multiplying the probabilities by a constant factor. With an eye to the conditional bigram frequencies of natural languages, see the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/Bigrams.html`, we choose a factor of 1000 and define the **conditional Bigram Log-Weight** (cBLW) of the bigram $s_i s_j$ by the formula

$$w_{ij} = \begin{cases} {}^{10}\log(1000 \cdot p_{j|i}) & \text{if } 1000 \cdot p_{j|i} > 1, \\ 0 & \text{otherwise} \end{cases} \qquad \text{for } i, j = 0, \ldots, n-1.$$

Given a family $\mathcal{B}$ of bigrams we define its **cBLW score** as

$$S_3(\mathcal{B}) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} k_{ij}(\mathcal{B}) \cdot w_{ij}$$

where $k_{ij}(\mathcal{B})$ is the number of occurrences of the bigram $s_i s_j$ in $\mathcal{B}$.

5 Bigram Frequencies

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/Bigrams.html`

6 The Values of Bigram Scores

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/cBLWsc.html`

Theoretical Values for Random Bigrams

Let $\Sigma = (s_0, \ldots, s_{n-1})$ be an alphabet and consider a probability distribution that assigns the probabilities p_i to the letters s_i. Choosing two letters independently from this distribution assigns the probability $p_i p_j$ to the bigram $s_i s_j$. Giving the bigrams whatever weights w_{ij} and scoring a set of bigrams by summing their weights the expected value of the weight of a bigram is

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} w_{ij} p_i p_j .$$

Using this formula with the letter and bigram frequencies of natural languages and the corresponding conditional bigram log-weights we get the table

English:	1.47	German:	1.54	French:	1.48

Theoretical Values for True Bigrams

For a "true" bigram we first choose the first letter s_i with probability p_i, then we choose the second letter s_j with conditional probability $p_{j|i}$. This assigns the probability $p_i p_{j|i} = p_{ij}$ to the bigram $s_i s_j$, and the expected conditional bigram log-weight is

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} w_{ij} p_{ij} .$$

Using this formula with the letter and bigram frequencies of natural languages and the corresponding conditional bigram log-weights we get the table

English:	1.94	German:	1.96	French:	1.99

Empirical Values for Natural Languages

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/cBLWsc.html`

7 A more systematic approach

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/Analysis2.html`

8 The Similarity of Columnar and Block Transpositions

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/Similar.html`

Permutation Matrices

Let $\sigma \in \mathcal{S}_p$ be a permutation of the numbers $1, \ldots, p$.

Let R be a ring (commutative with 1). Then σ acts on R^p, the free R-module with basis

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad e_p = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

as the linear automorphism

$$\rho(\sigma) \quad \text{defined by} \quad \rho(\sigma)e_i = e_{\sigma i}.$$

This gives an injective group homomorphism

$$\rho \colon \mathcal{S}_p \longrightarrow GL(R^p).$$

How to express $\rho(\sigma)$ as a matrix? The vector

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = x_1e_1 + \cdots + x_pe_p$$

maps to

$$\rho(\sigma)x = x_1e_{\sigma 1} + \cdots + x_pe_{\sigma p} = \begin{pmatrix} x_{\sigma^{-1}1} \\ \vdots \\ x_{\sigma^{-1}p} \end{pmatrix}.$$

Thus the matrix P_σ corresponding to $\rho(\sigma)$ is given by

$$P_\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}1} \\ \vdots \\ x_{\sigma^{-1}p} \end{pmatrix} \quad \text{for all } x \in R^p.$$

Therefore

$$P_\sigma = (a_{ij})_{1 \le i,j \le p} \quad \text{where} \quad a_{ij} = \begin{cases} 1, & \text{if } i = \sigma j, \\ 0 & \text{otherwise.} \end{cases}$$

Hence the matrix P_σ has exactly one 1 in each row and in each column, all other entries being 0. We call P_σ the **permutation matrix** belonging to σ.

Matrix Description of a Block Transposition

The permutation σ defines a block transposition f_σ over the alphabet $\Sigma = \mathbb{Z}/n\mathbb{Z}$: For $(a_1, \ldots, a_p) \in \Sigma^p$ let

$$f_\sigma(a_1, \ldots, a_p) = \left[P_\sigma \begin{pmatrix} a_1 \\ \vdots \\ a_p \end{pmatrix} \right]^T = (a_{\sigma^{-1}1}, \ldots, a_{\sigma^{-1}p}).$$

This moves the i-th letter a_i of the block to position σi.

More generally let $r = pq$ and $a = (a_1, \ldots, a_r) \in \Sigma^r$. Then

$$c = f_\sigma(a) = (a_{\sigma^{-1}1}, \ldots, a_{\sigma^{-1}p}, a_{p+\sigma^{-1}1}, \ldots, a_{p+\sigma^{-1}p}, \ldots, a_{(q-1)p+\sigma^{-1}p}).$$

From this we derive the general encryption formula:

$$c_{i+(j-1)p} = a_{\sigma^{-1}i+(j-1)p} \quad \text{for } 1 \le i \le p, 1 \le j \le q.$$

We may express this in matrix notation writing the plaintext as a matrix with $a_{i+(j-1)p}$ in row i and column j:

$$A = \begin{pmatrix} a_1 & a_{p+1} & \ldots & a_{(q-1)p+1} \\ \vdots & \vdots & a_{i+(j-1)p} & \vdots \\ a_p & a_{2p} & \ldots & a_{qp} \end{pmatrix} \in M_{p,q}(\mathbb{Z}/n\mathbb{Z}).$$

Analogously we write the ciphertext as $C \in M_{p,q}(\mathbb{Z}/n\mathbb{Z})$ where $C_{ij} = c_{i+(j-1)p}$ for $1 \le i \le p$, $1 \le j \le q$.

Then the encryption formula simply is the matrix product:

$$C = P_\sigma A$$

with the permutation matrix P_σ.

Matrix Description of a Columnar Transposition

The permutation σ also defines a columnar transposition g_σ over the alphabet $\Sigma = \mathbb{Z}/n\mathbb{Z}$: Writing the plaintext row by row in a $q \times p$-matrix gives just the transposed matrix A^T (again assume $r = pq$):

$$\begin{array}{cccccccc} & & & & & \downarrow & & \downarrow \\ \to & a_1 & \ldots & a_p & & a_{\sigma^{-1}1} & \ldots & a_{\sigma^{-1}p} \\ \to & a_{p+1} & \ldots & a_{2p} & \mapsto & a_{p+\sigma^{-1}1} & \ldots & a_{p+\sigma^{-1}p} \\ & \vdots & a_{(\mu-1)p+\nu} & \vdots & & \vdots & a_{(\mu-1)p+\sigma^{-1}\nu} & \vdots \\ \to & a_{(q-1)p+1} & \ldots & a_{qp} & & a_{(q-1)p+\sigma^{-1}1} & \ldots & a_{(q-1)p+\sigma^{-1}p} \end{array}$$

and the ciphertext is read off, as the little arrows suggest, column by column in the order given by σ. Thus the encryption function is given by:

$$\tilde{c} = g_\sigma(a_1, \ldots a_r) = (a_{\sigma^{-1}1}, a_{p+\sigma^{-1}1}, \ldots, a_{\sigma^{-1}p}, \ldots, a_{(q-1)p+\sigma^{-1}p}).$$

The encryption formula is:

$$\begin{aligned} \tilde{c}_{\mu+(\nu-1)q} &= a_{(\mu-1)p+\sigma^{-1}\nu} \quad \text{for } 1 \le \mu \le q, 1 \le \nu \le p \\ &= c_{\nu+(\mu-1)p}. \end{aligned}$$

If we arrange $\tilde{c}$ column by column as a matrix

$$\tilde{C} = \begin{pmatrix} \tilde{c}_1 & \tilde{c}_{q+1} & \ldots & \tilde{c}_{(p-1)q+1} \\ \vdots & \vdots & \tilde{c}_{\mu+(\nu-1)q} & \vdots \\ \tilde{c}_q & \tilde{c}_{2q} & \ldots & \tilde{c}_{pq} \end{pmatrix} \in M_{q,p}(\mathbb{Z}/n\mathbb{Z}),$$

we see that

$$\tilde{C}^T = C = P_\sigma A.$$

This shows:

Proposition 1 *The result of the columnar transposition corresponding to $\sigma \in \mathcal{S}_p$ on Σ^{pq} arises from the result of the block transposition corresponding to σ by writing the latter ciphertext in p rows of width q and transposing the resulting matrix. This produces the former ciphertext in q rows of width p.*

In particular columnar transposition and block transposition are similar.

(The proposition describes the required bijection of Σ^* for strings of length pq.)

For texts of a length not a multiple of p this observation applies after padding up to the next multiple of p. For a columnar transposition with an uncompletely filled last row this does not apply. In spite of this we assess columnar and block transpositions as similar, and conclude: Although a columnar transposition permutes the text over its complete length without period, and therefore seems to be more secure at first sight, it turns out to be an *illusory complication.*