# A pictorial illustration of conventional cryptography

Lars Ramkilde Knudsen

March 1993

**Abstract**

In this paper we consider conventional cryptosystems. We illustrate the differences between substitution, transposition and product ciphers by showing encryptions of a highly redundant cleartext, a portrait. Also it is pictorially demonstrated that no conventional cryptosystem in its basic mode provides sufficient security for redundant cleartexts.

## 1 Introduction

The history of cryptography is long and goes back at least 4,000 years to the Egyptians, who used hieroglyphic codes for inscription on tombs [2]. Since then many ciphers have been developed and used. Many of these old ciphers are much too weak to be used in applications today, because of the tremendous progress in computer technology. Until 1977 all ciphers were so-called *one-key ciphers* or *conventional ciphers*. In these ciphers the keys for encryption and decryption are identical or easily derived from each other. In 1977 Diffle and Hellman introduced *two-key ciphers* or *public-key ciphers*, where the knowledge of one key gives no knowledge about the other key. In this paper we consider only conventional ciphers. We divide these ciphers into three groups: Substitution Ciphers, Itansposition Ciphers and Product Ciphers. For each group we consider a specific cipher and give a pictorial

illustration of an encryption. Finally we give an illustration that the strong conventional cipher, DES, in its basic mode is insufflcient to ensure protection when used on a large plaintext.
Notation:
Let $\mathcal{A}_\mathcal{M}$ and $\mathcal{A}_\mathcal{C}$ be the alphabets for plaintexts and ciphertexts, respectively. Let $M = m_0, m_1, \ldots, m_{n-1}$ be a $n$-character plaintext, s.t. for every $i$, $m_i \in \mathcal{A}_\mathcal{M}$ and let $C = c_0, c_1, \ldots, c_{n-1}$ be a ciphertext, s.t. for everv $i, c \in \mathcal{A}_\mathcal{C}$

# 2 Substitution systems

As indicated in the name every plaintext character is substituted by some ciphertext character. There are four kinds of substitution ciphers.

- Simple substitution
- Polyalphabetic substitution
- Homophonic substitution
- Polygram substitution

We restrict ourselves to consider the first two kinds.

## 2.1 Simple substitution

In a cipher with a simple substitution each plaintext character is transformed into a ciphertext character via the same function **f. More formally,** $\forall i$ : $0 \leq i < n$

$$\mathbf{f} : \mathcal{A}_\mathcal{M} \rightarrow \mathcal{A}_\mathcal{C}$$
$$c_i = \mathbf{f}(m_i)$$

**As an example the following**

### 2.1.1 Caesar substitution

It is believed that Julius Caessr encrypted messages by shifting every letter in the plaintext 3 positions to the right in the alphabet. This cipher is based on ***shifted alphabets***, i.e. $\mathcal{A}_\mathcal{M} = \mathcal{A}_\mathcal{C}$, and is in general defined as follows

$$\mathbf{f(m_i)} = \mathbf{m_i} + \mathbf{k} \pmod{\mid \mathcal{AM} \mid}$$

For the Caesar cipher the secret key $k$ is the number $3$. In general, the cipher is easily broken in at most $\mid \mathcal{AM} \mid$ trials. Shift the ciphertexts one position until the Plaintext arises.

## 2.2 Polyalphabetic substitution

In a polyalphabetic substitution the plaintext characters are transformed into ciphertext characters using a $j$-character key $K = k_0, \ldots, k_{j-1}$, which defines $j$ distinct functions $\mathbf{F_{k_0}} \ldots, \mathbf{F_{k_{j-1}}}$. More formally $\forall i : 0 < i \leq n$

$$\begin{array}{ll} \mathbf{f_{kl}} & : \ \mathcal{A}_\mathcal{M} \rightarrow \mathcal{A}_\mathcal{C} \forall l : 0 \leq l < j \\ c_i & = \mathbf{f_{k_{imodj}}(m_i)}. \end{array}$$

As an example the following

### 2.2.1 The Vigenere cipher

The Vigenere cipher was first published in 1586. In 1917 in an article in Scientific American the cipher was claimed to be "impossible of translation" [Denning].
Let us assume again that $\mathcal{A}_\mathcal{M} = \mathcal{A}_\mathcal{C}$ Then the Vigenere cipher is defined as follows

$$c_i = \mathbf{f_{k_{imodj}}(m_i)} = \mathbf{m_i} + \mathbf{k_{imodj}} \pmod{\mid \mathcal{A}_\mathcal{M} \mid}$$

Vigenere ciphers can be broken when enough ciphertext is available to the cryptanalyst (index of coincidence, Kasiski's method).

# 3 Transposition systems

**Transposition systems are essentially permutations of the plaintext characters. Therefore $\mathcal{A}_\mathcal{M} = \mathcal{A}_\mathcal{C}$. A transposition cipher is defined as follows $\forall i : O \leq i < n$**

$$\begin{array}{lcl} \mathbf{f} & : & \mathcal{A}_\mathcal{M} \rightarrow \mathcal{A}_\mathcal{M} \\ \eta & : & \{0, \ldots, (n-1)\} \rightarrow \{0, \ldots, (n-1)\} \textbf{ a permutation} \\ c_i & : & \mathbf{f}(\mathbf{m_i}) = \mathbf{m}_{\eta(\mathbf{i})} \end{array}$$

**Many transposition ciphers permute characters with a fixed period $j$. In that case**

$$\begin{array}{lcl} \mathbf{f} & : & \mathcal{A}_\mathcal{M} \rightarrow \mathcal{A}_\mathcal{M} \\ \eta & : & \{0, \ldots, (j-1)\} \rightarrow \{0, \ldots, (j-1)\} \textbf{ a permutation} \\ c_i & : & \mathbf{f}(\mathbf{m_i}) = \mathbf{m}_{(\mathbf{i div j})+\eta(\mathbf{i mod j})} \end{array}$$

**A convenient way to express the permutation $\eta(i)$ in easily memorable form is by a key word. The alphabetic order of the key characters then defines the permutation. For example the key K=LARS would represent the permutation $\eta(i) = \{1, 0, 2, 3\}$. Consider the following transposition cipher**

## 3.1 Row transposition cipher

**Let the key be $K = k_1, \cdots, k_d$. The plaintext is divided into blocks of $d$ characters, and each block is permuted according to the alphabetic order of the characters in the key. Let us consider an example:**
***Example*: Let $d = 4$, the key $K = IVAN$ and the plaintext**

M = NOTASTRONGCIPHER

| $I$ | $V$ | $A$ | $N$ |
|---|---|---|---|
| 1 | 3 | 0 | 2 |
| $O$ | $A$ | $N$ | $T$ |
| $T$ | $O$ | $S$ | $R$ |
| $G$ | $I$ | $N$ | $C$ |
| $H$ | $R$ | $P$ | $E$ |

**The ciphertext is**

**C = OANTTOSRGINCHRPE**

**We can do slightly better with the same key by combining row transposition with columnar transposition. Consider**

## 3.2 Row and columnar transposition ciphers

**Let the key be $K = k_1, \ldots, k_d$. The plaintext is divided into blocks of $d \times d$ characters. Each block is written into a $d \times d$ matrix by rows according to the alphabetic order of the characters in the key. Then the ciphertexts is read from the matrix by columns according again to the alphabetic order of the characters in the key, thus the period of the cipher becomes $d^2$. Let us consider an example:**
***Example*: Let $d = 4$, the key K=IVAN and the plaintext**

**M = NOTASTRONGCIPHER**

**M = NOTASTRONGCIPHER**

| | | $I$ | $V$ | $A$ | $N$ |
|---|---|---|---|---|---|
| | | 1 | 3 | 0 | 2 |
| $I$ | 1 | $O$ | $A$ | $N$ | $T$ |
| $V$ | 3 | $T$ | $O$ | $S$ | $R$ |
| $A$ | 0 | $G$ | $I$ | $N$ | $C$ |
| $N$ | 2 | $H$ | $R$ | $P$ | $E$ |

The ciphertext read out from the matrix is

C = GINCOANTHRPETOSR

l ansposition ciphers can be broken, however, using tables of frequency distribution for digrams and trigrams.

# 4 Product systems

An obvious attempt to make stronger ciphers than the ones we've seen so far, is to combine substitution and transposition ciphers. These ciphers are called product cipher. Many product ciphers has been developed, including Rotor machines. We restrict ourselves to a short description of the most famous product cipher ever developed.

## 4.1 Data Encryption Standard

In 1977 (15.01.77) the National Bureau of Standards in the U.S. published the Data Encryption Standard (DES). The DES consists of 16 rounds of permutations and substitutlons. The DES encrypts 64 bit plaintexts into 64 bit ciphertexts using a 56 bit key. It Is beyond the scope of this paper to go further into details about the construction of the DES. We refer to the references in this paper. The basic mode of DES, the Electronic Code Book (ECB) Mode, is defined as follows

$$c_i = DES_k(m_i)$$

In other words $c_i$ is the 64 bit encrypted value of the 64 bit plaintext $m - i$ using the 56 bit key $k$. The next section illustrates, that this mode is insufficient to ensure protection when used on a large plaintext. For this purpose the Cipher Block Chaining (CBC) Mode is recommended

$$c_i = DES_k(m_i \oplus c_{i-1})$$

where $c_1$ is a fixed constant and $\oplus$ is bitwise addition modulo 2. The best known attack on DES so far was published in 1991 by E. Biham and A. Shamir [Biham]. It finds the secret key, but requires $2^{47}$ chosen plaintexts. This is a very weak and unrealistic attack. In favour of the DES it should be noted, that the attacks on the ciphers mentioned in the preceding two Sections are known ciphertext attacks. These ciphers are trivially broken in a chosen plaintext attack.

# 5 The illustrations

We consider the encryptions of a data-file 'FRAZETTA'. The file consists of 22080 characters of each 8 bits and is pictured in Figure 1. As can be seen the file contains redundancy. The Figures 2-7 show the ciphertexts obtained by using the ciphers discussed earlier. The one-time pad is the only cipher, which is perfect in the sense of Shannons theory. The cipher is defined as follows

$$c_i = m_i \oplus k_i$$

The obvious disadvantage is the long key. For 'FRAZETTA' we need a 22080 byte key. Figure 8 is a ciphertext obtained using the one-time pad and is included for comparison.

## 5.1 Comments on the figures

Ad. Fig. 2-5: These four figures illustrates that the four ciphers do not provide sufficient protection. The redundancy in the plaintext is more or less transferred to the ciphertexts. Ad. Fig. 6: In order to illustrate the inadequacy of the ECB Mode only blocks of 8 bits ($m_i$) are encrypted. That is, let $8msb$ be a function that returns the 8 most significallt bits of a message. The ciphertext in Fig. 7 is defined

$$c_i = 8msb(DES_k(m_i \parallel 56 \textbf{ zeros}))$$

**Note that although protection is not obtained, the key remains secret, in contrast to the ciphers in Fig. 2-5.**
**Ad. Fig. 7: In order to illustrate the effect of using CBC instead of ECB, this ciphertext is defined**

$$c_i = 8msb(DES_k(m_i \oplus c_{i-1} \parallel 56 \textbf{ zeros}))$$

**Ad. Fig. 8: The ideal ciphertext.**

**For illustrations order hardcopy.**

# References


**[Denning] D. E. Denning.(1982)**
**Crvptography and Data Security.**
**Addison-Wesley Pnblishing Company, Inc.**

**[David] D.W. Davies and W.L. Price (1989)**
**Security for Computer Networks**
**John Wiley & Sons**

**[Biham] Eli Biham, Adi Shamir (1976)**
**Differential Cryptanalysis of the full 16-Tound DES.**
**Technical Report # 708,**
**Technion - Israel Institute of Technology.**