Fundamentals of Information & Network Security
ECE 471/571

Lecture #6: Early Ciphers and Cryptanalysis

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Vigenere Cipher

- Best known polyalphabetic cipher. Key is m-length vector. Use different monoalphabetic substitutions as one proceeds through the plaintext message

$$y = e_K(x_1, x_2, .., x_m) = (x_1 + K_1, x_2 + K_2, .., x_m + K_m) \bmod 26,$$
$$d_K(y_1, y_2, .., y_m) = (y_1 - K_1, y_2 - K_2, .., y_m - K_m) \bmod 26.$$

Example: key: “deceptive”; plaintext: “we are discovered save yourself”, obtain the ciphertext:

```
key:            deceptivedeceptivedeceptive
plaintext:      wearediscoveredsaveyourself
ciphertext:     ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Hill Cipher

- Takes *m* successive plaintext letters and substitutes for them *m* ciphertext letters
- The substitution is determined by *m* linear equations in which each character is assigned a numerical value

$\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ K must be invertible $e_K(x) = \underline{x}K,$ $d_K(y) = \underline{y}K^{-1}.$

- For example:

plaintext: test $K = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}$

- Question: Is the Hill cipher encryption an injective function?

Stream Ciphers

- Generate a keystream z = $z_1 z_2 \cdots$ and encrypt each character x_i of the plaintext with a different key z_i.

$$y = y_1 y_2 \cdots = e_{z_1}(x_1) e_{z_2}(x_2) \cdots$$

- Shift and Vigenere ciphers can be viewed as special cases of stream cipher
- Vernam Cipher
- One-Time Pad
  - Key is as long as the message

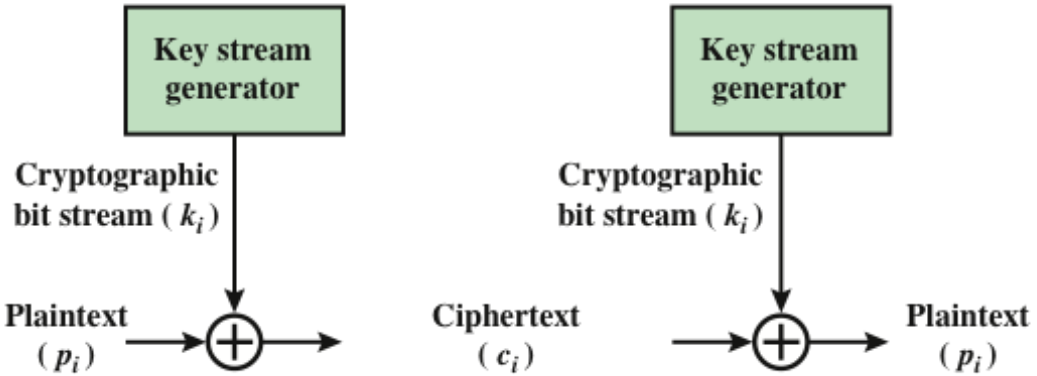


Figure 3.7 Vernam Cipher

Permutation Ciphers

- Permutation (transposition)
  - Rearranging of the symbols, a.k.a Permutation
  - Diffusion: widely spreading the information from the message or the key across the ciphertext
  - Break the establish pattern

- Formal definition: $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$

$$y = e_\pi(x_1, ..., x_m) = (x_{\pi(1)}, ..., x_{\pi(m)})$$
$$x = d_\pi(y_1, ..., y_m) = (y_{\pi^{-1}(1)}, ..., y_{\pi^{-1}(m)}).$$

j	1	2	3	4	5	6
$\pi(j)$	3	5	1	6	4	2

j	1	2	3	4	5	6
$\pi^{-1}(j)$	3	6	1	5	2	4

Example: plaintext is: followashore

Permutation (cont'd)

- Rail Fence Cipher
  - Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows

Plaintext: m e m a t r h t g p r y
e t e f e t e o a a t

Ciphertext: MEMATRHTGPRYETEFETEOAAT

- Columnar Transpositions
  - A rearrangement of the characters of the plain text into columns

- Example

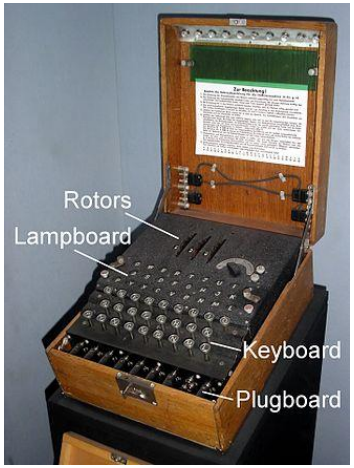
Plaintext: We are discovered. Flee at once.

W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E					

Ciphertext: WIREEESEAACDTROFOEVLNDEEC

Cryptanalysis

- The goal of cryptanalysis?



The Enigma machine

Question: should the crypto algorithms be published or not?

Kerckhoffs' principle

Auguste Kerckhoffs (1883):

The enemy knows the system

The cipher should remain secure even if **the adversary knows the specification of the cipher.**

The only thing that is **secret** is a

short key **k**

that is **usually chosen uniformly at random**

Kerckhoffs' Principle – the Motivation

1. In commercial products it is unrealistic to assume that the design details remain secret (**reverse-engineering!**)

2. Short keys are easier to **protect**, **generate** and **replaced**.

3. The design details can be discussed and **analyzed in public**.