Cryptography is making of cryptosystems. Cryptanalysis is breaking of Crypto systems. Cryptology is Cryptography and Cryptanalysis.

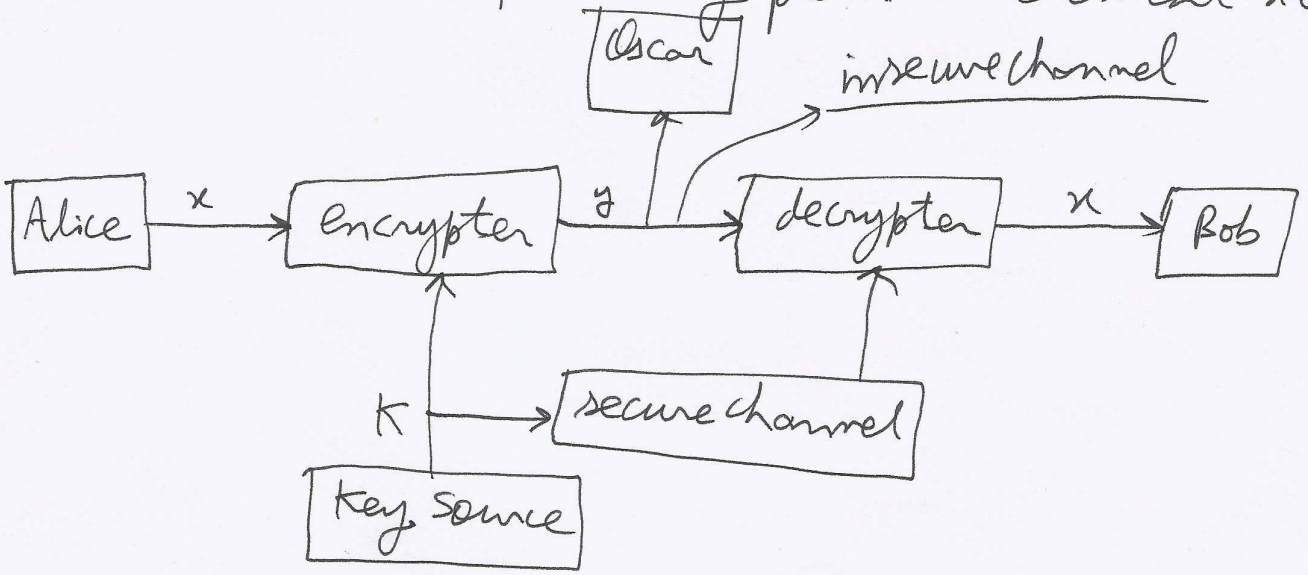
A Cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

(1) $\mathcal{P}$ is a finite set of possible plaintexts;

(2) $\mathcal{C}$ is a finite set of possible ciphertexts;

(3) $\mathcal{K}$, the Keyspace, is a finite set of possible keys;

(4) For each $k \in \mathcal{K}$, there is an encryption rule $e_k \in \mathcal{E}$ and a corresponding decryption rule $d_k \in \mathcal{D}$. Each $e_k : \mathcal{P} \to \mathcal{C}$ and $d_k : \mathcal{C} \to \mathcal{P}$ are functions such that $d_k(e_k(x)) = x$ for every plaintext element $x \in \mathcal{P}$.



The communication channel

The Shift Cipher: let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. For $0 \le k \le 25$, define $e_k(x) = (x + k) \pmod{26}$, and $d_k(x) = (y - k) \pmod{26}$ for $x, y \in \mathbb{Z}_{26}$.

For the particular key $k = 3$, the cryptosystem is called the Caesar Cipher, which was used by Julius Caesar.

We convert alphabets modulo 26 as follows:

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

Example: Suppose the key for a Shift Cipher is $k = 11$, and the plaintext is: wewillmeetatmidnight.

We first convert the plaintext to a sequence of integers:

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19

Next, we add 11 to each value, reducing each sum mod 26:

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

Finally, we convert the sequence of integers to alphabetic characters, obtaining the ciphertext: HPHTWWXPPELE XTOYTRSE.

To decrypt the ciphertext, Bob will first convert the ciphertext to a sequence of integers, then subtract 11 from each value (reducing mod 26), and finally convert the sequence of integers to alphabetic characters.

The Substitution Cipher: Let $P = C = Z_{26}$, K consists of all possible permutations of the 26 symbols $0, 1, \ldots 25$. For each permutation $\pi \in K$, define $e_\pi(x) = \pi(x)$, and define $d_\pi(y) = \pi^{-1}(y)$, where π^{-1} is the inverse permutation to π.

Example: Consider the permutation π:

a→X, b→N, c→Y, d→A, e→H, f→P, g→O, h→G, i→Z, j→Q, k→W, l→B, m→T, n→S, o→F, p→L, q→R, r→C, s→V, t→M, u→U, v→E, w→K, x→J, y→D, z→I

Here we have $e_\pi(a) = X$, $e_\pi(b) = N$, etc. The plaintext "wewillmeetatmidnight" will be encrypted as: KHKZBBTHHMXMTZAS2OGM. For decrypting the message, we make use of the inverse permutation π^{-1}:

A→d, B→l, C→r, D→y, E→v, F→o, G→h, H→e, I→z, J→x, K→w, L→p, M→t, N→b, O→g, P→f, Q→j, R→q, S→n, T→m, U→u, V→s, W→k, X→a, Y→c, Z→i.

Here we have, $d_\pi(A) = d$, $d_\pi(B) = l$, etc.

The shift cipher is a special case of the Substitution Cipher which includes only 26 of the 26! possible permutations of 26 elements. Another special case of the Substitution Cipher is the Affine Cipher.

The Affine Cipher: Let $P = C = \mathbb{Z}_{26}$ and let

$K = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a,26) = 1\}$.

For $K = (a,b) \in K$, define $e_K(x) = (ax+b) \pmod{26}$ and $d_K(y) = a^{-1}(y-b) \pmod{26}$ for $x, y \in \mathbb{Z}_{26}$.

Example: Let $K = (7,3)$. $7^{-1} \pmod{26} = 15$. We have $e_K(x) = 7x+3 \pmod{26}$, and $d_K(y) = 15(y-3) = 15y - 19 \pmod{26}$

Suppose the plaintext is: "we will meet at midnight."

The corresponding numbers mod 26 are:

22 4 22 8 11 11 12 4 4 19 0 19 12

8 3 13 8 6 7 19

Applying the transform $e_K(x) = 7x+3 \pmod{26}$, we get:

1 5 1 7 2 2 9 5 5 6 3 6 9

7 24 16 7 19 0 6

We get the corresponding ciphertext as:

~~A F A H B B J F F G~~

B F B H C C J F F G D G J H Y Q H T A G

In all of the previous crypto systems: Shift Cipher, Substitution Cipher, and Affine Cipher, once a key is chosen, each alphabetic character is mapped to a unique alphabetic character. For ~~those~~ this reason, these cryptosystems are called **monoalphabetic cryptosystems**. Using the correspondence $A \to 0$, $B \to 1$, ... $Z \to 25$ described earlier, we can associate each key K with an alphabetic string of length m, called a **keyword**. The **Vigenere Cipher** encrypts m alphabetic characters at a time: each plaintext element is equivalent to m alphabetic characters.