Chiffrement par substitution

Algo. de chiffrement par substitution :

$$\begin{aligned}
&\mathcal{P} = \mathcal{C} = \mathbb{Z}, \mathcal{K} = \{\pi/\pi \text{ permutation sur } \mathbb{Z}\},\\
&\forall \pi \in \mathcal{K}, x, y \in \mathbb{Z}, (\pi^{-1} \circ \pi = \pi \circ \pi^{-1} = id),\\
&e_\pi(x) = \pi(x),\\
&d_\pi(y) = \pi^{-1}(y).
\end{aligned}$$

Propriétés : par bloc, monoalphabétique, à clé privée, idempotent et $|\mathcal{K}| = 26! > 4 * 10^{26}$.

Attaque : fréquence des lettres.

Exemple : Déchiffrement de

$$\begin{aligned}
y = \quad & RUZVFSMLXCMZVQFDHUJLF\\
& UCAHVYFUCVHVBFZSMXZSHV
\end{aligned}$$

par la substitution :

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

Chiffrement par substitution (suite)

lem.: Le système de chiffrement par substitution offre une confidentialité parfaite.

Algo. de chiffrement affine :

$$\begin{aligned}
&\mathcal{P} = \mathcal{C} = \mathcal{K} = \{(a,b) \in \mathbb{Z} * \mathbb{Z} / pgcd(a,26) = 1\},\\
&\forall k = (a,b) \in \mathcal{K}, x, y \in \mathbb{Z},\\
&e_k(x) = ax + b \; mod \; 26,\\
&d_k(y) = a^{-1}(y-b) \; mod \; 26.
\end{aligned}$$

Attaque : recherche exhaustive de la clé
($|\mathcal{K}| = 26 * \phi(26) = 312$).

Chiffrement par décalage : $a = 1$.

Exemple : Déchiffrement par décalage ($b = 11$) :

$$\begin{aligned}
y = \; & ZSNZXMTPYOPXLCTYDN\\
& ZXMTPYOPNLATELTYPD
\end{aligned}$$

Chiffrement de Hill

Algo. de chiffrement de Hill :

$$\mathcal{P} = \mathcal{C} = (\mathbb{Z})^m,$$
$$\mathcal{K} = \{\text{matrices } m * m \text{ inversibles dans } \mathbb{Z}\},$$
$$\forall K \in \mathcal{K}, x, y \in (\mathbb{Z})^m,$$
$$e_K(x) = xK,$$
$$d_K(y) = yK^{-1}$$

Remarque : une matrice de $\mathbb{Z}_m$ est inversible ssi $pgcd(det\ K, m) = 1$.

Propriétés : par bloc, polyalphabétique, idempotent et à clé privée.

Exemple : Chiffrer puis déchiffrer $x = et$ avec
$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, $K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

Chiffrement de Hill (suite)

Chiffrement par permutation :

$$\mathcal{K} = \{\pi/\pi \text{ permutation sur } \mathbb{Z}_m\},$$
$$\forall \pi \in \mathcal{K}, x = x_1 \ldots x_m, y = y_1 \ldots y_m \in \mathbb{Z}^m,$$
$$(\pi^{-1} \circ \pi = \pi \circ \pi^{-1} = id),$$
$$e_\pi(x) = x_{\pi(1)} \cdots x_{\pi(m)},$$
$$d_\pi(y) = y_{\pi^{-1}(1)} \cdots y_{\pi^{-1}(m)}.$$

$$K_\pi = (k_{ij})/k_{ij} = \begin{cases} 1 & \text{si } i = \pi(j) \\ 0 & \text{sinon} \end{cases}$$

Chiffrement de Vigénère ($XVI^{ème}$) et de Vernam (1917)

Algo. de chiffrement de Vigénère :

$$\begin{array}{l}\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z})^m, \\ \forall K, x, y \in (\mathbb{Z})^m, \\ K = k_1 \ldots k_m, x = x_1 \ldots x_m, y = y_1 \ldots y_m, \\ e_K(x) = (x_1 +_{26} k_1) \ldots (x_m +_{26} k_m) \ (\ mod\ m), \\ d_K(y) = (y_1 -_{26} k_1) \ldots (y_m -_{26} k_m) \ (\ mod\ m).\end{array}$$

Propriétés : en chaine périodique de période m, polyalphabétique, à clé privée, idempotent et $|\mathcal{K}| = 26^m$.

Algo. de chiffrement de Vernam :

$$\begin{array}{l}\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^m, \\ \forall x, y, k \in (\mathbb{Z}_2)^m, e_k(x) = x \oplus k, d_k(y) = y \oplus k,\end{array}$$

lem.: Les systèmes de chiffrement de Vigénère et de Vernam offrent une confidentialité parfaite.