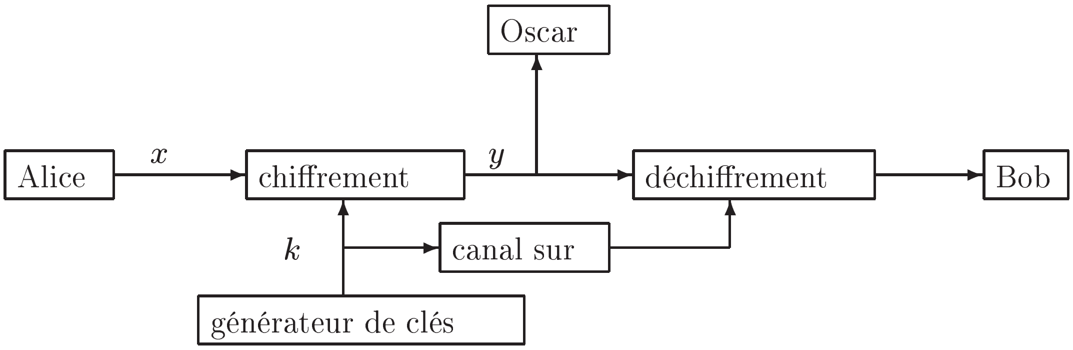
Définition d'un système cryptographique



Le tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ est un système cryptographique si :

$\mathcal{P}$:	Ensemble des textes clairs ;
$\mathcal{K}$:	Ensemble des clés ;
$\mathcal{C}$:	Ensemble des textes chiffrés ;
$\mathcal{E}$:	Ensemble des règles de chiffrement pour les clés de $\mathcal{K}$;
$\mathcal{D}$:	Ensemble des règles de déchiffrement pour les clés de $\mathcal{K}$;
Et :	$\forall k \in \mathcal{K}, \exists e_k \in \mathcal{E}, \exists d_k \in \mathcal{D}, \forall x \in \mathcal{P}$, $d_k(e_k(x)) = x$.

La cryptanalyse

principe de Kerckhoff : Oscar connait le système cryptographique utilisé.

but : Déterminer la clé utilisée.

Les attaques :
- Texte chiffré connu : Oscar ne connait que la chaine du message chiffré.
- Texte clair connu : Oscar dispose d'un texte clair et du texte chiffré correspondant.
- Texte clair choisi : Oscar a accès à une machine chiffrante.
- Texte chiffré choisi : Oscar a temporairement accès à une machine déchiffante.

Typologie des systèmes

Clé privée/clé publique :
- clé privée : la totalité de la clé est communiqué en secret (Chiffrement par substitution, de Hill, de Vigénère, le DES,...) ;
- clé publique : une partie de la clé est communiquée en secret tandis que l'autre est communiquée en publique (RSA, chiffrement de Rabin,...).

Chiffrement par bloc/en chaine :
- par bloc : la clé ne varie pas au cours du chiffrement ;
- en chaine : la clé varie au cours du chiffrement.

Monoalphabétique/polyalphabétique :
- monoalphabétique : pour un caractère clair, un caractère chiffré ;
- polyalphabétique : pour un caractère clair, plusieurs caractères chiffrés ;

Système idempotent ou non

Chiffrement en chaine

Le tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F}, \mathcal{E}, \mathcal{D})$ est un système cryptographique en chaine si :

$\mathcal{P}$: Ensemble des textes clairs ;
$\mathcal{K}$: Ensemble des clés ;
$\mathcal{C}$: Ensemble des textes chiffrés ;
$\mathcal{L}$: Alphabet de séquence de clés ;
$\mathcal{F}$: $(f_1, f_2, \dots)$ générateur de séquence : $\forall i \leq 1, f_i : \mathcal{K} * \mathcal{P}^{i-1} \rightarrow \mathcal{L}$;
$\mathcal{E}$: Ensemble des règles de chiffrement pour les clés de $\mathcal{L}$;
$\mathcal{D}$: Ensemble des règles de déchiffrement pour les clés de $\mathcal{L}$;
Et : $\forall z \in \mathcal{L}, \exists e_z \in \mathcal{E}, \exists d_z \in \mathcal{D}, \forall x \in \mathcal{P}$, $d_z(e_z(x)) = x$.

Si la séquence ne dépend que de la clé : système synchrone.

Si $\forall i \geq 1, z_i = z_{i+d}$: système périodique.

rem.: Si $\forall i \geq 1, z_i = K$: chiffrement par bloc.

Système cryptographique produit

Principe : combiner les systèmes cryptographiques.

but : augmenté la sécurité des systèmes.

Soient $S_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$ et $S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$ deux systèmes cryptographiques. Le système $S = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1 * \mathcal{K}_2, \mathcal{E}, \mathcal{D})$ défini par

$$\begin{array}{l} \forall k = (k_1, k_2) \in \mathcal{K}_1 * \mathcal{K}_2, \forall x, y \in \mathcal{P} \\ e_{(k_1,k_2)}(x) = e_{k_2}(e_{k_1}(x)), \\ d_{(k_1,k_2)}(y) = d_{k_1}(d_{k_2}(y)) \end{array}$$

est le système produit (noté $S_1 * S_2$).

S^n est le système cryptographique itéré.

Un système S est idempotent si $S^2 = S$.