Cryptographie et Sécurité - TD5

guillaume.postic@universite-paris-saclay.fr

Exercice 1 : chiffrement authentifié

Le mode CCM combine le mode CTR pour le chiffrement et le CBC-MAC pour l'authentification. Il est seulement défini pour des chiffrements par blocs de 128 bits (comme AES), mais nous travaillerons sur des blocs de 3 bits pour cet exercice.

Calculer le chiffrement en mode CCM

- du message clair $\boldsymbol{m} = \texttt{011011011}$,
- avec des données authentifiées additionnelles $\mathbf{AAD} = \texttt{100011}$,
- et le *nonce* choisi pour ce message $\boldsymbol{nonce} = \boldsymbol{Compteur} = \texttt{010}$,
  qui est égal au premier bloc compteur, par souci de simplification.

Le chiffrement par bloc de 3 bits est défini dans la table ci-dessous :

Entrée	Sortie	Entrée	Sortie
000	001	100	010
001	100	101	110
010	111	110	011
011	000	111	101

Exercice 2 : générateur congruentiel linéaire

Le générateur congruentiel linéaire (GCL) est un exemple très simple de PRNG. Il génère une séquence de nombres pseudo-aléatoire, chacun calculé par récurrence :

$$X_{n+1} \equiv a \cdot X_n + c \pmod{m},$$

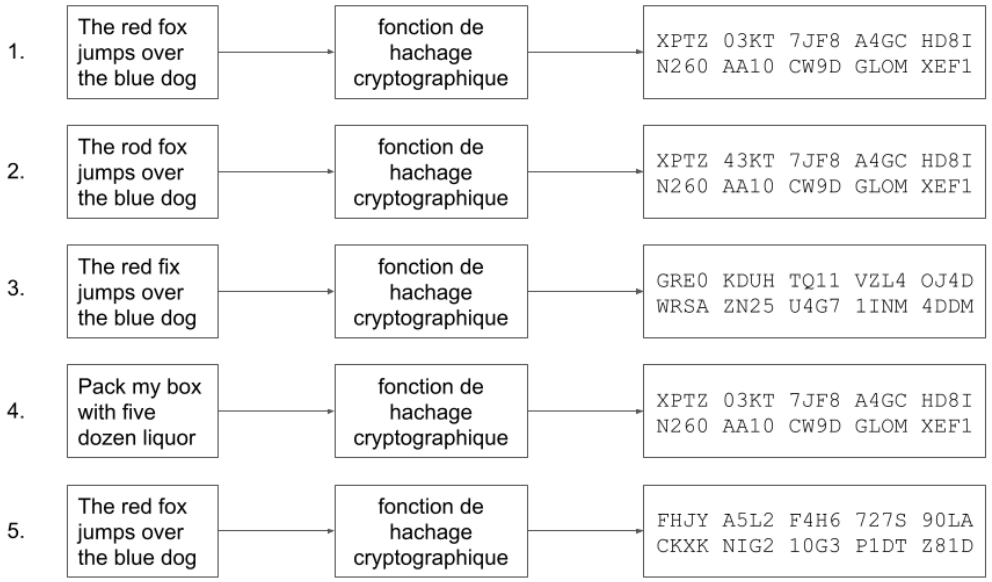
avec

- X_n est le nombre d'indice n,
- X_0 est l'état initial du générateur (*i.e.* le nombre d'indice 0),
- a, c et m sont des constantes.

Calculer X_{23} pour $X_0 = 0$, $a = 2$, $c = 2$ et $m = 5$.

Exercice 3 : fonction de hachage cryptographique

Identifier les problèmes de la fonction de hachage illustrée ci-dessous :



Exercice 4 : code d'authentification de message de hachage à clé

Calculer le HMAC du message m = `10110110`, avec

- la clé secrète K = `1100`,
- $ipad$ = `1111`,
- $opad$ = `0000`,
- la fonction de hachage $h(X) = \mathbf{bin}(\Sigma x_i \bmod 16)$