

TD 5 : Révision cryptographie symétrique

Question de cours :

1. Définir la cryptographie symétrique. Quels sont ses avantages et ces inconvénients par rapport à la cryptographie asymétrique ?
2. Quelles sont les exigences de sécurité possibles ? L'attaquant ne peut pas...

Chiffrement par flux :

3. Rappelez la définition d'une fonction aléatoire, donnez un exemple. Pourquoi utilise-t-on la fonction aléatoire dans la crypto symétrique.
4. Donner la définition formelle d'une sécurité inconditionnelle. Quelle est la probabilité dans un masque jetable, pour que quelque soit le message on a $E(k,m)=c$?
5. Comment casse-t-on un masque jetable en pratique?
6. Peut-on prouver la sécurité d'un chiffrement de flux en pratique?

Chiffrement par blocs :

1. Quels sont les deux principes fondamentaux sur lesquelles le chiffrement par blocs se reposent, qui ont été introduite par Shannon. Explicitez chaque notions.
2. Quel est le rôle de table substitution « S-box » dans le chiffrement par blocs ?

Chiffrement DES :

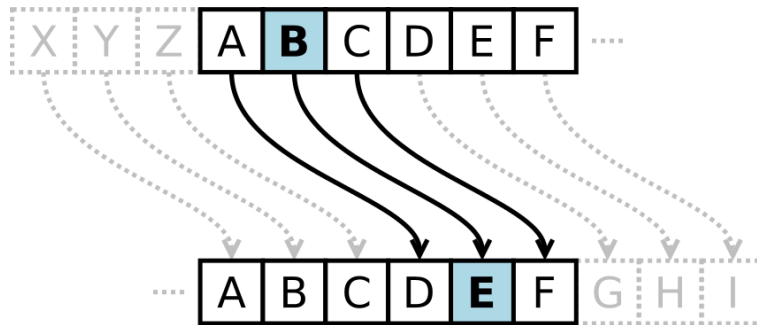
1. Comment la fonction aléatoire est appliquée dans le chiffrement DES de telle façon que le résultat soit réversible ?
2. Rappelez le théorème de Luby-Rackoff
3. Quels sont les 2 propriétés de sécurité qu'un chiffrement DES doit satisfaire ?
4. Comment le simple DES a été attaqué ?
5. Pourquoi le double DES est à proscrire ? Expliquez les deux techniques d'attaques utilisées.

Chiffrement AES :

1. Décrivez les différentes étapes d'un tour d'un AES ?
2. Combien de tour pour un AES de 128 bits ?
3. Quelle est la principale différence entre la boîte S-box d'un chiffrement DES avec celle d'un chiffrement AES ?
4. Quelles sont les 2 principales attaques contre la S-box d'un AES ?

1 exercice

Le chiffrement de César, ou chiffrement à décalage, est un système à substitution mono-alphabétique où chaque lettre du message en clair est décalée d'un pas constant. L'image suivante issue Wikipedia illustre le procédé dans le cas d'un décalage de 3 lettres.



1. S'agit-il d'un chiffrement à flux ou à bloc ? Combien existe-t-il de secrets pour ce chiffrement ?
2. On souhaite chiffrer le texte « Attaquez, maintenant ! ». Préciser les pré-traitements à effectuer avant de chiffrer le message et calculer son chiffré avec la clef 6.
3. Expliquer la procédure de déchiffrement et déchiffrer dwwdtxhpcdlqwhqdqw avec la clef 3.
4. Sachant qu'un chiffré est issu d'un clair en français, expliquer comment casser le code de César en utilisant un argument sur la fréquence des lettres.
5. Déchiffrer le message jlzabullupntl.
6. On propose une modification du chiffre de César où l'on utilise non plus un décalage à pas constant mais une bijection quelconque de l'alphabet dans lui-même. Comparer le nombre de clefs possibles dans ce cas au précédent. L'analyse fréquentielle est-elle encore envisageable ?