Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 3.23

Magenta (pour *Multifunctional Algorithm for General-purpose Encryption and Network Telecommunication Applications*) est un algorithme de chiffrement par bloc qui a été soumis à la compétition AES par *Deutsch Telekom AG*. Il s'agit d'un schéma de Feistel à 6 tours qui chiffre des blocs de 128 bits avec une clé de 128 bits. La clé K est divisée en deux sous-clés K_1 et K_2 de 64 bits chacune et la fonction de tour est notée F. La clé K_1 est utilisée dans la fonction F pour les tours 1, 2, 5 et 6 et la clé K_2 est utilisée dans les tours 3 et 4.

Exercice 3.23 ATTAQUE PAR DISTINGUEUR SUR Magenta

En utilisant un moyen pour distinguer un schéma de Feistel à deux tours d'une permutation aléatoire (par une attaque à clairs choisis), proposer une attaque (indépendamment de la fonction de tour utilisée) à clairs et chiffrés choisis contre le système de chiffrement Magenta qui demande 2^{64} clairs choisis, 2^{64} chiffrés choisis et un coût algorithmique équivalent à 2^{64} évaluations de l'algorithme de chiffrement.

Solution : La clé K_1 est utilisée dans les deux premiers et les deux derniers tours du chiffrement et un attaquant peut faire une recherche exhaustive sur K_1 indépendamment de K_2 en utilisant le distingueur contre un schéma de Feistel à deux tours pour trouver la bonne clé K_1.

Pour distinguer un schéma de Feistel à deux tours, il suffit d'obtenir deux couples de clair/chiffré (P_1, C_1) et (P_2, C_2) où les parties droites des deux clairs sont identiques (*i.e.* $P_1^R = P_2^R$) et de vérifier que $C_1^R \oplus C_2^R = P_1^L \oplus P_2^L$ (*cf.* Exercice (**??**)).

Étant donné un message clair X_0, un attaquant peut demander le chiffrement X_6 de X_0 pour la clé K inconnue. Pour chaque clé $\tilde{K_1}$ possible de 64 bits, il calcule le chiffrement partiel de deux tours de X_0 et obtient une valeur X_2. Il construit un élément X_2' tel que $X_2^R = X_2'^R$ et calcule le déchiffrement partiel de X_2' noté X_0' pour la clé $\tilde{K_1}$. Il demande ensuite le chiffrement X_6' de X_0' sous la clé K. Il effectue ensuite le déchiffrement partiel de X_6 et de X_6' sous la clé K_1' pour obtenir X_4 et X_4'. Si la clé $\tilde{K_1}$ est égale à la sous-clé K_1 de K, alors X_4 (*resp.* X_4') est le chiffré de X_2 (*resp.* X_2') par un schéma de Feistel à deux tours utilisant la clé K_2. Puisque que $X_2^R = X_2'^R$, si $\tilde{K_1} = K_1$, la relation $X_4^R \oplus X_4'^R = X_2^L \oplus X_2'^L$ est satisfaite indépendamment de la clé K_2.

La liste des clés pour lesquelles cette relation est vérifiée ne contiendra que quelques éléments (éventuellement filtrés en répétant l'attaque avec un autre chiffré) et pour chacun d'eux l'attaquant pourra effectuer une recherche exhaustive pour trouver la clé K_2.

Déterminer la clé K_1 demande quatre applications de la fonction F par clé testée (soit $4/6$ du coût du chiffrement de Magenta) et trouver la clé K_2 demande deux applications de la fonction F par clé testée (soir $2/6$ du coût du chiffrement de Magenta). Le coût total de l'attaque correspond donc à 2^{64} évaluations complètes de l'algorithme de chiffrement et demande un clair choisi et un chiffré choisi par test de la clé K_1. □