M2 IDL parcours GLIA
Année universitaire 2015-2016

Administration réseau et sécurité – partie Network Security (première session)

Autorisés : documents manuscrits, notes de cours imprimées du site web, dictionnaires papiers.
Interdits : livres, téléphones portables, calculatrices, traducteurs électroniques.

1. Cryptanalyse différentielle de DES (5 points)

La figure 1 montre la S-box 3 de DES. On peut voir que $S_3(110110)=12_{10}$ (car la ligne est *1----0* et la colonne est *-1011-*).

S_3	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
01	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
10	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
11	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Figure 1 : La S-box 3 de DES.

Question 1.1 (0.5 point) : Quelle est la valeur de $S_3(010101)$ en décimal ?
Question 1.2 (0.5 point) : Combien y a-t-il d'entrées possibles pour S_3 ?
Question 1.3 (4 points) : Posons $O_1=S_3(I_1)$ et $O_2=S_3(I_2)$. Faisons l'hypothèse que $I_1 \oplus I_2=000001$ (où $\oplus$ représente l'opération XOR), et que $O_1 \oplus O_2=1100$. Nous faisons l'hypothèse que I_1 est compris entre 0 et 15_{10} (pour réduire le nombre de valeurs à vérifier). Quelles sont les valeurs possibles de I_1 (parmi ces 16 valeurs) ?

2. Cryptographie à courbes elliptiques (5 points)

La figure 2 représente la courbe elliptique d'équation $y^2=x^3-x+1$. Posons $A=(1,1)$, $B=(0,-1)$ et $C=(3,-5)$.

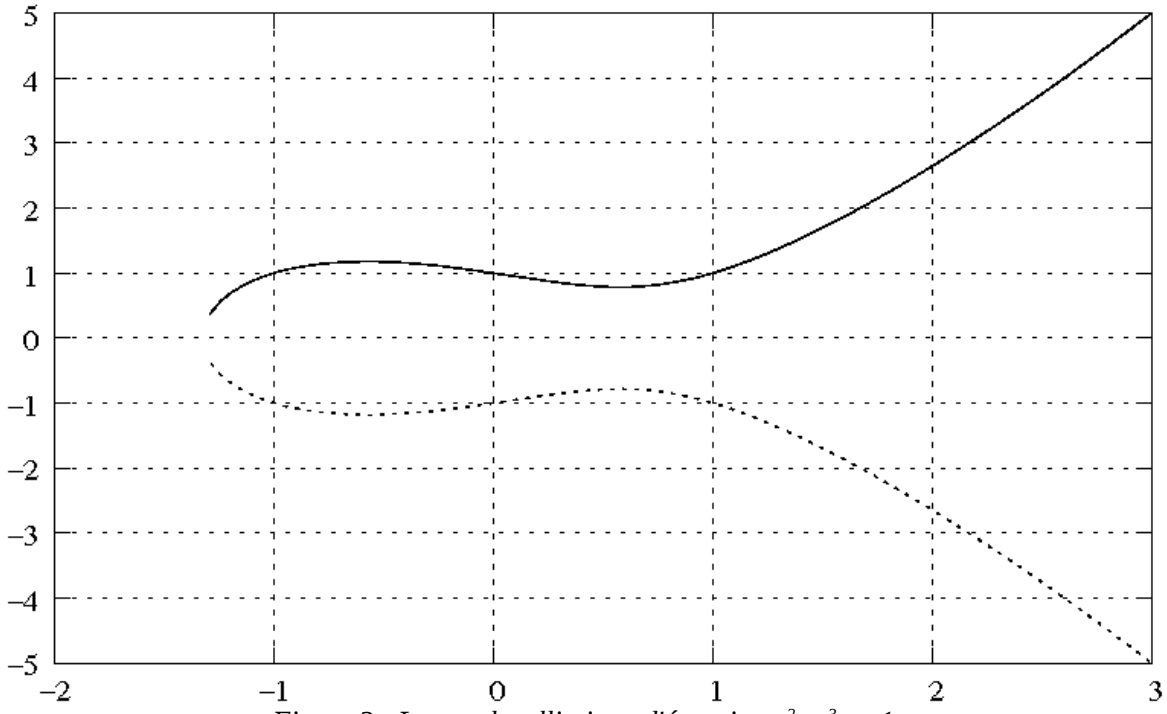

Figure 2 : La courbe elliptique d'équation $y^2=x^3-x+1$.

Question 2.1 (1 point) : Dessinez le point $A+B$.
Question 2.2 (1 point) : Dessinez le point $2A$.
Question 2.3 (1 point) : Dessinez le point $3A$.
Question 2.4 (1 point) : Dessinez le point $B+C$.
Question 2.5 (1 point) : Dessinez le point $4C$.

3. Attaques sur WEP (10 points)

L'algorithme WEP *(Wired Equivalent Privacy)* [1] était utilisé dans les versions initiales de IEEE 802.11 pour fournir de la confidentialité. WEP utilise une clé secrète k partagée entre deux entités qui communiquent. Pour transmettre des données d, les opérations suivantes sont effectuées : un vecteur d'initialisation aléatoire iv de 24 bits est généré, une somme de contrôle $c(d)$ est calculée (indépendemment de k), le message chiffré $C=(d+c(d))\oplus RC4(iv,k)$ est calculé, où + représente la concaténation et ⊕ l'opération XOR, et $iv+C$ est envoyé. Dans la suite, nous décrivons des attaques présentées dans [2].

Question 3.1 (1 point) : Pourquoi est-il nécessaire de fournir de la confidentialité dans les communications sans fil ? Quelle est l'utilité du vecteur d'initialisation ? Quelle est l'utilité de la somme de contrôle (à part l'intégrité basique) ?
Question 3.2 (1 point) : Expliquez comment le message chiffré est décrypté et vérifié.
Question 3.3 (1 point) : Le standard WEP recommande de changer le vecteur d'initialisation à chaque message. Quel est la durée pour qu'un même vecteur d'initialisation soit réutilisé, si un point d'accès envoie des paquets de 1000 octets à 5 Mbps ?
Question 3.4 (1 point) : Si P_1 et P_2 sont deux messages clairs (avec la somme de contrôle), et C_1 et C_2 sont les deux messages chiffrés correspondants, encodés avec le même iv, montrez que $C_2=C_1\oplus P_1\oplus P_2$.
Question 3.5 (2 points) : Supposons qu'un attaquant connaît un message clair P_1 et le message chiffré correspondant iv_1+C_1. Montrez qu'il est alors possible à l'attaquant de calculer un message chiffré valide pour des données d_2.
Question 3.6 (1 point) : Proposez une manière d'éviter cette attaque.

Question 3.7 (2 points) : Nous faisons à présent l'hypothèse que l'attaquant dispose de deux messages chiffrés avec le même vecteur d'initialisation.

- Expliquez comment obtenir le contenu du deuxième message chiffré, à partir de la connaissance du premier message clair.
- Les auteurs de [2] indiquent que “L'attaquant peut (…) envoyer des emails aux utilisateurs et attendre qu'ils les consultant sur un lien sans fil.”. Expliquez pourquoi cela permet à un attaquant de connaître le contenu du premier message chiffré, et donnez les hypothèses requises.

Question 3.8 (1 point) : Dans le cas où aucun message clair n'est connu, il est souvent possible d'obtenir des informations sur les messages clairs. Pour justifier cela, les auteurs de [2] disent que “Plusieurs champs d'un trafic IP sont prédictibles, puisque les protocoles utilisent des structures bien définies dans les messages, et les contenus des messages sont fréquemment prédictibles.”. Justifiez cela au travers d'un exemple, et donnez les hypothèses requises.

4. Références

[1] IEEE Computer Society. “Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Standard 802.11, Édition de 1999, 1999.
[2] N. Borisov, I. Goldberg, D. Wagner. “Intercepting mobile communications: The insecurity of IEEE 802.11.”, dans les actes de ACM MOBICOM, 2011.