

Réseau et sécurité – Examen terminal - deuxième session

Exercice 1 : Cryptanalyse du chiffrement de Vigenère (6 points)

Soit le texte suivant traitant du coronavirus (extrait de Wikipedia), et chiffré avec Vigenère par une clé inconnue K (les espaces ne sont pas significatifs et servent uniquement à faciliter le décompte des lettres) :

xaxsb qqmqw rrood arret cfscm nlwav qdcfs zmliv wrunn wqgue cksry ezysa feihd rxemd
ozmli vwrmc wjcam vqjif aukgj vppzg jbcum wdndl mucea ninwe gsasf foodw zyqax hoemi
bdsaa vmepe qdfig ympzg jvzcm vsugb masao hqfsp qnbjo yqebh zhpez wqvee uwbgp avkzn
hitds qqwcx oabuf kgrbr whotq difgy qmwfr rqnba se

Question 1.1 (4 points) : Quelle est la taille de la clé K ? Expliquez votre résultat.

Question 1.2 (2 points) : Expliquez les raisons qui pourraient faire que la taille K que vous obtenez ne serait pas la bonne ? Avez-vous cependant confiance dans la valeur obtenue ?

Exercice 2 : Attaque sur la signature RSA-sans-hachage (6 points)

Soit (n, d) une clé privée RSA et (n, e) la clé publique correspondante. La signature d'un message m avec RSA-sans-hachage est $m^d \pmod n$. Pour vérifier la signature s d'un message m , on teste si l'égalité $s^e = m \pmod n$ est vérifiée.

Question 2.1 (2 points) : Supposons que l'attaquant connaisse la signature de deux messages m_1 et m_2 . Montrez que l'attaquant peut produire la signature du message $m_1 m_2$.

Question 2.2 (2 points) : Supposons que l'attaquant veuille créer une signature valide pour un message m_3 . Supposons qu'il puisse faire signer des messages qu'il choisit à Alice, tant qu'ils sont différents de m_3 . Montrez comment il procède pour obtenir la signature de m_3 .

Question 2.3 (2 points) : En quoi l'ajout de la fonction de hachage empêche cette attaque ?

Exercice 3 : Attaque sur la signature El Gamal (8 points)

Le mécanisme de signature de El Gamal est le suivant : soit p un nombre premier et g un entier (générateur). La clé privée est un entier a tel que $0 < a < p-1$ et a premier avec $p-1$. La clé publique est le triplet $(p, g, y = g^a \pmod{p-1})$. La signature d'un message m est le couple $(r, s) = (g^k \pmod{p-1}, k^{-1}(h(m) - a \cdot r) \pmod{p-1})$, avec k une valeur aléatoire. La vérification de la signature se fait en testant l'égalité $y^r \cdot r^s = g^{h(m)} \pmod{p}$.

Question 3.1 (4 points) : Montrez que la signature (r, s) d'un message m peut être vérifiée. On admettra que puisque g est premier avec p , alors $b = c \pmod{p-1}$ équivaut à $g^b = g^c \pmod{p}$.

Question 3.2 (4 points) : Montrez que si deux messages m_1 et m_2 sont signés avec la même valeur aléatoire k , alors on peut en déduire la clé a .