Université de Perpignan C. Negre – C. Mouilleron

TD 3 Arithmétique et Cryptographie à clef publique
Cryptographie à clef publique

Exercice 1. Calculer

- $13 \times 7 \mod 17$, puis $13 + 7 \mod 17$, puis $123^7 \mod 179$.
- $\text{pgcd}(434, 128)$ et une relation de Bezout correspondante.

Exercice 2. Combien d'opérations (nombre de multiplications et mise au carré modulo N) sont nécessaires pour un chiffrement RSA avec l'exposant $k = 2^{16} + 1$?

Exercice 3. Soit $n \geq n' \geq 0$ deux entiers. Rappelons que durant l'algorithme d'Euclide une suite de reste de division euclidienne sont calculés comme suit

$$r_i = q_{i+2} r_{i+1} + r_{i+2}$$

et $r_0 = n, r_1 = n'$.

1. Montrer par récurence sur i que $r_i \geq 2r_{i+2}$.
2. Soit k tel que r_k soit le dernier r_i non nul (k est égal au nombre de division euclienne effectuer pendant l'algorithme d'Euclide). Montrer que k est $O(\log n)$.

Exercice 4 (Echange de clef de Diffie Hellman)**.** Soit $p = 251$ et le générateur $g = 11$. Soit maintenant $n_A = 15$ et $n_B = 21$. Déterminer la clef commune à Alice et Bob, s'ils effectuent un échange de clef de Diffie-Hellman.

Exercice 5 (ElGamal)**.** Soit $p = 53, g = 2, B = 30$ la clef publique ElGamal de Bob.

- Chiffrez le message $m = 42$ avec la clef publique de Bob. On prendra 17 comme nombre aléatoire pour le chiffrement.
- On suppose que la clef secrète de Bob est 13. Vérifiez le et déchiffez le message ($r = 15, c = 17$).

Exercice 6 (Chiffrement RSA)**.** Soit $N = 989$ un entier RSA, et $m = 534$. Chiffrer le message m avec la clef $k = 23$. Déchiffrer le avec la clef de déchiffrement $k' = 683$ (vous vérifierez au préalable que $k \times k' \mod (p-1)(q-1) = 1$ où $p = 23$.

Exercice 7 (Signature RSA)**.** Soit Bob qui a construit un cryptosystème RSA, les données publiques sont $N = 989$ et $k = 23$ les données privées sont $p = 23, q = 43$ et $k' = 683$.

Pour signer un message m, Bob calcule $s = m^{k'} \mod N$. Une personne qui souhaite vérifier que s est bien la signature de Bob calcule $s^k \mod N$, qui vaut m si la signature est correcte.

Calculer la signature RSA (sans fonction de hachage) de $m = 123$.

Exercice 8. Montrer que le chiffrement RSA ne résiste pas aux attaques à texte chiffré choisi. En particulier étant donné un texte chiffré y, montrer comment choisir un texte chiffré $\hat{y} \neq y$ tel que la connaissance du texte clair $\hat{x} = d_k(\hat{y})$ permette de calculer $x = d_k(y)$.

(Indication : utiliser le fait que $e_k(x_1)e_k(x_2) \mod N = e_k(x_1 x_2 \mod N)$).

Exercice 9. Cet exercice présente un exemple d'*échec de protocole* dans lequel un texte chiffré peut être décrypté par un opposant sans déterminer la clef, à cause d'une mauvaise utilisation du système cryptographique. Il faut en conclure qu'il n'est pas suffisant d'avoir un système cryptographique sur pour garantir la confidentialité de la communication.

Supposons que Bob utilise le chiffrement RSA avec un modulus N assez grand pour qu'il soit impossible de le factoriser. Supposons qu'Alice envoie à Bob un message dans lequel chaque caractère alphabétique est représenté par un nombre de 0 à 25 ($A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$). Alice chiffre chaque lettre du message séparément.

1. Décrire comment Oscar peut facilement décrypter un message chiffré de cette façon.
2. Illustrer l'attaque en décryptant le texte chiffré suivant, obtenu avec le chiffrement RS avec les paramètres $N = 18721$ et $k = 25$, sans factoriser le modulo.

$$365, 0, 4845, 14930, 2608, 2608, 17173.$$

Exercice 10. Supposons qu'Alice utilise le schéma de signature d'ElGamal. Afin d'économiser du temps dans la génération des nombres aléatoires r qui sont utilisés pour signer les messages, Alice choisit une valeur aléatoire initiale r_0, puis signe le i-eme message en utilisant la valeur $r_i = r_0 + 2i \mod (p-1)$ (par conséquent $r_i = r_{i-1} + 2 \mod (p-1)$ pour tout $i \geq 1$).

1. Supposons que Bob observe deux messages signés consécutifs $(x_i, sign(x_i))$ et $(x_{i+1}, sign(x_{i+1}))$. Décrire comment Bob peut alors facilement calculer la clef secrète d'Alice a sans résoudre une instance du problème du logarithme discret. (Remarquer que la valeur de i n'a pas besoin d'être connue pour que l'attaque réussisse.)
2. Supposons que les paramètres du schéma soient $p = 28703, g = 5, A = 11339$ et que l'es deux messsages observés par Bob soient

$$\begin{array}{rcl} x_i = 12000, & sign(x_i, r_i) & = (26530, 19862) \\ x_{i+1} = 24567, & sign(x_i, r_i) & = (3081, 7604) \end{array}$$

   Trouver la valeur de a en utilisant l'attaque décrite précédemment.

Exercice 11. Comment deux cryptogrammes ElGamal peuvent être utilisés pour générer le troisième cryptogramme ElGamal d'un message clair inconnu? Comment peut-on empecher cette attaque?

Exercice 12 (Schnorr)**.** Vérifier sur un exemple que le protocole de Schnorr fonctionne correctement.