# 16 PRATIQUE PROCÉDURALE 2

### Déroulement de l'activité

| Description | Début | Fin | Durée |
|---|---|---|---|
| | | | |

*Le contenu du guide de l'étudiante et de l'étudiant pour cette activité suit. Les solutions et les directives y sont ajoutées.*

**But de l'activité**

Étudier différentes solutions aux problèmes de sécurité étudiés (canaris, stack non-exécutable, tunnels VPN), comprendre comment on utilise la méthode de chiffrement RSA.

## 16.1 Virtual Private Networks (VPNS)

Vous avez fort probablement déjà utilisé des réseaux virtuels privés (RVP en français, VPN en anglais), par exemple pour vous connecter aux serveurs internes de l'université à partir de la maison. Les questions qui suivent se rapportent à ce type de solution aux problèmes de la visibilité des paquets sur le réseau internet.

a. Sur le réseau internet, les communications chiffrées font souvent usage de deux types de chiffrement, l'un de type RSA, et l'autre de type AES. Par exemple, Alice va produire une clé AES, la chiffrer avec la clé publique RSA de Bob, et lui envoyer cette clé chiffrée. De son côté, Bob fera de même. Pourquoi procède-t-on de cette façon ? RSA permet l'échange d'information sécurisée sans échange sécurisé préalable. Cependant, c'est une méthode qui exige beaucoup de calculs. Par contre, les méthodes de chiffrement symétriques (comme AES, Blowfish, etc.) sont beaucoup plus performantes que RSA, mais exigent un échange préalable sécurisé de la clé symétrique utilisée. L'utilisation conjointe des deux systèmes donne donc une système idéal : pas de distribution de clé de façon sécurisée préalable, système d'encryptage performant.
b. Qu'arrive-t-il si Ève envoie à Alice une clé publique RSA en prétendant que cette clé provient de Bob ? Ève pourra par la suite intercepter les messages de Alice destinés à Bob et les décrypter.
c. Comment Ève pourrait-elle écouter la communication entre Alice et Bob sans que ceux-ci ne le sachent ? Ève intercepte l'envoi de la clé publique de Bob à Alice Ève envoie sa propre clé publique à Alice Ève intercepte le message de Alice destiné à Bob qui contient la clé AES encrypté avec la clé publique qu'Alice croit être celle de Bob

Ève décrypte le message d'Alice, conserve une copie de la clé AES, la réencrypte avec la vraie clé publique de Bob, et lui envoie le tout Bob obtient la clé AES encryptée en croyant qu'elle provient directement d'Alice, la décrypte avec sa propre clé privée, et commence à échanger des messages encryptés AES avec Alice en utilisant la clé AES qu'il vient de recevoir Alice et Bob échange de l'information encryptée AES en croyant être à l'abri Ève subtilise des copies de ces messages, et peut les décrypter à l'aide de la clé AES dont elle a une copie.

d. Que peut-on faire pour empêcher Ève de procéder ainsi ? On utilise un "Certificate Authority" (CA), duquel on connaît avec certitude la clé publique. Dans les systèmes d'exploitation modernes, les clés publiques de certains CA sont incluses. Les clés publiques des sites reconnus sont échangées de façon sécurisée entre le site et le CA. Le CA va ensuite signer la clé publique avec sa propre clé privée. Lorsqu'on obtient la clé publique d'un site, on peut donc valider si cette clé est authentique, parce qu'on peut vérifier qu'elle est reconnue par un CA valide.

## 16.2 RSA - Considérations théoriques

Lorsqu'on fait des calculs de modulo avec des nombres ayant de très gros exposants, on décompose l'exposant en multiples de 2, et on utilise des modulos de nombres intermédiaires (par exemple, $V^4 \mod (n) = ((V^2 \mod (n)) \times (V^2 \mod (n))) \mod (n)$).

a. Soit : $V = kn + r$, avec $V$, $k$, $n$ et $r$ entiers, et $r < V$ ; Pouvez-vous prouver que $V^2 modulo(n) = r^2 modulo(n)$ ? On peut faire cette preuve de 2 façons différentes :

   1. Puisque $V = kn + r$, alors $V^2 = (kn + r)^2 = k^2n^2 + 2knr + r^2 \mod n = r^2 \mod n$ (puisque tous les multiples de $n$ sont nuls modulo $n$)
   2. Puisque $V = kn + r$, alors $V \mod n = r + (kn \mod n = 0)$ Alors, $V^2 \mod n = r^2 \mod n$

b. Soit : $T = UW$, avec $T, U, W$ entiers. Prouvez que $T \mod (n) = ((U \mod (n)) \times (W \mod (n))) \mod (n)$ Posons $U = k_1n + r_1$, et $W = k_2n + r_2$.

   Alors :

   $T = UW = k_1k_2n^2 + (k_1r_2 + k_2r_1)n + r_1r_2$

   $T \mod n = r_1r_2 \mod n$ (puisque les multiples de $n$ sont nuls modulo $n$)

   Or, $U \mod n = r_1$, $W \mod n = r_2$, d'où :

   $T \mod n = r_1r_2 \mod n = ((U \mod n) \times (W \mod n)) \mod n$

## 16.3 Chiffrement Diffie-Hellman

Dans cette question, nous étudions l'impact du choix de $p$ et $g$ sur la sécurité de la méthode Diffie-Hellman. Pour aider votre réflexion dans cette question, vous pouvez observer le tableau des puissances de ($g \mod 17$) utilisé lors du premier procédural.

a. Soit $q$ un très grand nombre premier, et $p = 2 \times p_1 \times p_2 \cdots \times p_k \times q + 1$ un autre nombre premier, avec $p_1, p_2, \ldots, p_k$ également des nombres premiers. Quelles sont les tailles des cycles de puissances possibles pour $g^x \mod p$, avec $1 \leq g < p$ et $x = 1, 2, 3, \ldots$ un nombre entier ? Comment pourrait-on valider que les puissances successives d'un certain $g$ forment un cycle de taille $t$ ? Les nombres $g$ ont des puissances avec des cycles de longueur bien précise, chacune un facteur du nombre $p - 1$. Donc pour $p = 2 \times p_1 \times p_2 \cdots \times p_k \times q + 1$, les longueurs de cycles sont de : 1, 2, $p_1$, ... $p_k$, $q$, ainsi que toutes les combinaisons de produits des facteurs premiers de $p - 1$.

   Si $g^t \equiv 1 \mod p$ et que $t$ est un nombre premier, alors les puissances de $g$ forment un cycle de $t$ valeurs distinctes.

b. Soit $p = 2 \times q + 1$, où $p$ et $q$ sont des nombres premiers. Quelles sont les longueurs possibles des cycles des puissances de $g$ (où $1 \leq g < p$) ? Le petit théorème de Fermat peut être utile pour répondre à cette question.

   Note : les nombres premiers $q$ pour lesquels $p = 2 \times q + 1$ est aussi un nombre premier sont appelés des nombres premiers de Sophie Germain en l'honneur de la mathématicienne française qui les a étudié. La longueur de chaque cycle est nécessairement un facteur de $p - 1$. Si $p = 2q + 1$, alors $p - 1 = 2 \times q$, dont les facteurs sont 1, 2, $q$ et $2q$. Dans ce cas, pour tout $g$ plus petit que $p$, le cycle des puissance est soit de longueur 1, soit de longueur 2, soit de longueur $q$, soit de longueur $2 \times q$. Il n'y a que le nombre 1 qui a un cycle de longueur 1. Comme la racine carrée de 1 modulo $p$ ne peut être que 1 ou $-1$, il n'y a que $p - 1$ qui peut avoir un cycle de puissance de longueur 2. Donc pour toutes les autres valeurs modulo $p$ (toutes les valeurs entières positives plus petites que $p$, sauf 1 et $p - 1$), la longueur des cycles est soit de $q$, soit de $2 \times q$. Pour un nombre premier $p$ avec ces caractéristiques, tout nombre $g$ est donc valable lorsqu'il est : $1 < g < p - 1$.

## 16.4 Chiffrement Diffie-Hellman 2

Vous recevez plusieurs triplets Diffie-Hellman d'un interlocuteur. Évaluez la validité de ces triplets, et expliquez vos réponses.

a. $(q, p, g) = (1237, 19801, 13)$ Les 4 conditions à vérifier pour s'assurer de la qualité des paramètres de la méthode Diffie-Hellman sont les suivants :

1. $q$ est un nombre premier
2. $p$ est un nombre premier
3. $p-1$ est un multiple de $q$ (c'est-à-dire, $p = 1 \bmod q$)
4. $g$ est acceptable (génère assez de puissances différentes : il faut vérifier que $g^q = 1 \bmod p$

Ici,

1. $q = 1237$ est premier,
2. $p = 19801$ est premier,
3. $p \bmod q = 9$ (ce n'est pas $1 mod q$)
4. $g^q \bmod p = 6094$ (ce n'est pas $1 \bmod p$)

$\Rightarrow$ Valeurs inacceptables

b. $(q, p, g) = (1007, 6043, 9)$

1. $1007 = 19 \times 53$ n'est pas premier
2. $p = 6043$ est premier
3. $p \bmod q = 1$
4. $g^q \bmod p = 1$

$\Rightarrow$ inacceptables

c. $(q, p, g) = (12347, 123471, 11)$

1. $123471 = 3 \times 3 \times 3 \times 17 \times 269$ n'est pas premier
2. $p = 123471$ est premier
3. $p \bmod q = 1$
4. $g^q \bmod p = 30731$

$\Rightarrow$ inacceptables

d. $(q, p, g) = (1009, 10091, 3)$

1. $q = 1009$ est premier
2. $p = 10091$ est premier
3. $p \bmod q = 1$
4. $g^q \bmod p = 1$

$\Rightarrow$ Ces valeurs sont acceptables

## 16.5 Factorisation - Méthode (p-1) de Pollard

Tentez de factoriser le nombre 482723 à l'aide de la méthode $(p-1)$ de Pollard. Pour ce faire, vous pouvez explorer les puissances successives du nombre 2 (beaucoup d'autres

nombres peuvent être utilisés, mais le calcul sera plus facile avec 2, puisque pour les premières élévations à une puissance, vous conserverez un nombre qui est un multiple de 2. Ceci devrait vous permettre de sauter quelques étapes de calcul (lesquelles, et pourquoi ?)

$2^1 \mod 482723 = 2 \rightarrow PGCD(482723, 2-1) = 1$

$2^3 \mod 482723 = 8 \rightarrow PGCD(482723, 8-1) = 1$

$8^4 \mod 482723 = 4096 \rightarrow PGCD(482723, 4096-1) = 1$

$4096^5 \mod 482723 = 240276 \rightarrow PGCD(482723, 240276-1) = 1$

$240276^6 \mod 482723 = 288237 \rightarrow PGCD(482723, 288237-1) = 241$

Alors $p = 241$ et $q = 482723/241 = 2003$