Sécurité Informatique

Chapitre 2 :

Cryptographie symétrique

(Moderne)

Guellil zouaoui

Cryptographie symétrique (Rappel)

- L’algorithme de cryptographie est publique
- Le processus de chiffrement/déchiffrement utilise la même clé.
- La clé est secrète, c'est-à-dire connue seulement de l'émetteur et du récepteur
- Problème : comment se mettre d'accord sur la clé au départ?=>problème de l'échange de clés

Échange de clés

- Le problème d'échange de clés provient du fait que les parties qui communiquent doivent en quelque sorte partager une clé secrète sur un canal de communication **non sécurisée**, et les deux parties doivent alors s'assurer que la clé reste secrète !
- Solution :
  - échange de clés par une réunion en face à face (pour n correspondant n(n-1)/2 est nécessaire !).
  - L'utilisation d'un service de messagerie de confiance.
  - L'envoi de la clé via un canal de chiffrement existant.
- Les deux premiers sont souvent impraticables et toujours dangereux, tandis que le troisième dépend de la sécurité d'un échange de clés précédent.

Échange de clés Diffie-Hellman (DH)

- Il est apparu pour la première fois en 1976, dans lequel Deffie et Hellman proposent une méthode spécifique pour effectuer la tâche d'échange de clés
- Il s'agit d'un protocole qui permet à deux groupes de personnes qui ne se connaissent pas déjà de créer une clé secrète partagée sur un canal **non sécurisé**.
- Méthode basée sur l'élévation à une puissance dans un champ fini.
- La sécurité réside dans la difficulté du problème du logarithme discret.

Diffie-Hellman (DH): principe

- Alice choisit deux nombres p et g (nombre public).
- P est premier et « g » une racine primitive modulo P.
- Alice choisit un nombre secret x et envoie à Bob (g,p, $A= g^x \bmod p$)
- Bob choisit un nombre secret y et envoie à Alice ($B=g^y \bmod p$) et calcule la clés $K= A^y \bmod p$
- Alice calcule la clé $K= B^x \bmod p$

Diffie-Hellman (DH): principe

- À la fin de l'échange, Alice et Bob disposent de la même clé secrète $K = g^{xy} \bmod p$, qu'ils ne se sont pas échangés directement.
- $B = g^{y} \bmod p$
- $A = g^{x} \bmod p$
- $A^{y} \bmod p = (g^{x})^{y} \bmod p = g^{xy} \bmod p = g^{yx} \bmod p = (g^{y})^{x} \bmod p = B^{x} \bmod p$

Définition :Primitif

- On définit une racine primitive d'un nombre premier *p*, un nombre dont les puissances modulo p génèrent des nombres de 1 à *p*-1.
- Si *a* est une racine primitive d'un nombre premier *p*, alors les nombres

  $a \bmod p, a^2 \bmod p, \ldots, a^{p-1} \bmod p$

  sont distincts et se composent des nombres entiers de 1 à p-1 (sans ordre).
- Remarque : Tous les nombres n'ont pas une racine primitive.

Définition :Primitif

- « g » une racine primitive modulo P si :

$$\forall \alpha \in (1..p-1)\ \exists \beta\ tel\ que\ g^{\beta} \equiv \alpha\ mod\ p$$

- L'exposant est appelé le logarithme discret

Le nombre 3 est une racine primitive modulo 7

$$\begin{aligned}
3^1 &= 3 = 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7 \\
3^2 &= 9 = 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod 7 \\
3^3 &= 27 = 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod 7 \\
3^4 &= 81 = 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod 7 \\
3^5 &= 243 = 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod 7 \\
3^6 &= 729 = 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod 7 \\
3^7 &= 2187 = 3^6 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7
\end{aligned}$$

les racines primitives modulo n pour n ≤ 72

n	racine primitive modulo n	n	racine primitive modulo n
1	0	37	2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35
2	1	38	3, 13, 15, 21, 29, 33
3	2	39	
4	3	40	
5	2, 3	41	6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35
6	5	42	
7	3, 5	43	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34
8		44	
9	2, 5	45	
10	3, 7	46	5, 7, 11, 15, 17, 19, 21, 33, 37, 43
11	2, 6, 7, 8	47	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45
12		48	
13	2, 6, 7, 11	49	3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47
14	3, 5	50	3, 13, 17, 23, 27, 33, 37, 47
15		51	
16		52	
17	3, 5, 6, 7, 10, 11, 12, 14	53	2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51
18	5, 11	54	5, 11, 23, 29, 41, 47
19	2, 3, 10, 13, 14, 15	55	
20		56	
21		57	
22	7, 13, 17, 19	58	3, 11, 15, 19, 21, 27, 31, 37, 39, 43, 47, 55
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21	59	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56
24		60	
25	2, 3, 8, 12, 13, 17, 22, 23	61	2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59
26	7, 11, 15, 19	62	3, 11, 13, 17, 21, 43, 53, 55
27	2, 5, 11, 14, 20, 23	63	
28		64	
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27	65	
30		66	
31	3, 11, 12, 13, 17, 21, 22, 24	67	2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63
32		68	
33		69	
34	3, 5, 7, 11, 23, 27, 29, 31	70	
35		71	7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69
36		72	

Diffie-Hellman : exemple

	Alice	Bob
Étape 1	Alice choisi deux nombres p=23 et g=5	
Étape 2	Alice choisi un nombre secret x=7 et envoie à Bob (p=23,g=5, A= 5^7 mod 23 = 17)	
Étape 3		Bob choisi un nombre secret 8 et envoie à Alice (B=5^8 mod 7=16) et calcule la clés K= 17^8 mod 7=18
Étape 4	Alice calcule la clés K= 16^7 mod 7 = 18	

Diffie-Hellman : sécurité (attaque passive)

- connaissant p,g, A et B il est impossible calculer la clés K comme le font Alice ou Bob, car il manque toujours l'une des informations nécessaires, à savoir x ou y.
- Impossible de retrouver x connaissant $A=g^x \bmod p$, g et p, puisque la résolution du logarithme discret est un problème difficile.
- Cette découverte de Diffie et Hellman est une vraie révolution dans l'histoire de la cryptographie.
- Le problème de l'échange des clés est en effet résolu.

Diffie-Hellman : sécurité (attaque passive)

- connaissant p,g, A et B il est impossible calculer la clés K comme le font Alice ou Bob, car il manque toujours l'une des informations nécessaires, à savoir x ou y.
- Impossible de retrouver x connaissant $A=g^x \bmod p$, g et p, puisque la résolution du logarithme discret est un problème difficile.
- Cette découverte de Diffie et Hellman est une vraie révolution dans l'histoire de la cryptographie.
- Le problème de l'échange des clés est en effet résolu.
- Ce protocole est vulnérable à « l'attaque de l'homme du milieu » (attaque active).

Diffie-Hellman : sécurité (attaque active)

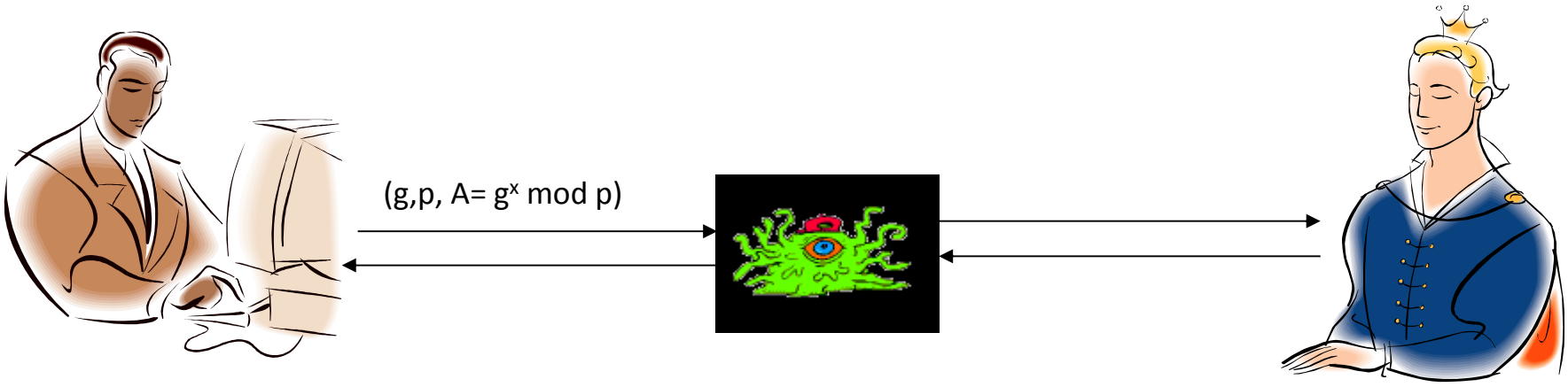
- L’attaque d'homme au milieu (MITM) est une forme d'écoute électronique dans laquelle des acteurs malveillants s'insèrent dans une conversation entre deux parties et interceptent des données via un canal de communication non sécurisé.
- L’attaquant divise la connexion d'origine en deux nouvelles connexions, l'une entre la première victime et l'attaquant et l'autre entre l'attaquant et la seconde victime.

Diffie-Hellman : sécurité (attaque active)

- Alice envoie à Bob g^a mod p.
  - Mais le message est intercepter par un acteur malveillant (**MITM)** qui envoie à Bob g^c mod p.
- Bob envoie à Alice g^b mod p.1
  - Mais le message va etre intercepter par **MITM** qui envoie à Alice g^d mod p.
- Alice calcule $(g^d)^a$ mod p.
- Bob calcule $(g^c)^b$ mod p.
- un canal de communication sécurisé est créer entre l'attaquant et Bob et un autre entre l'attaquant et Alice.

Diffie Hellman

- Man in the middle attack



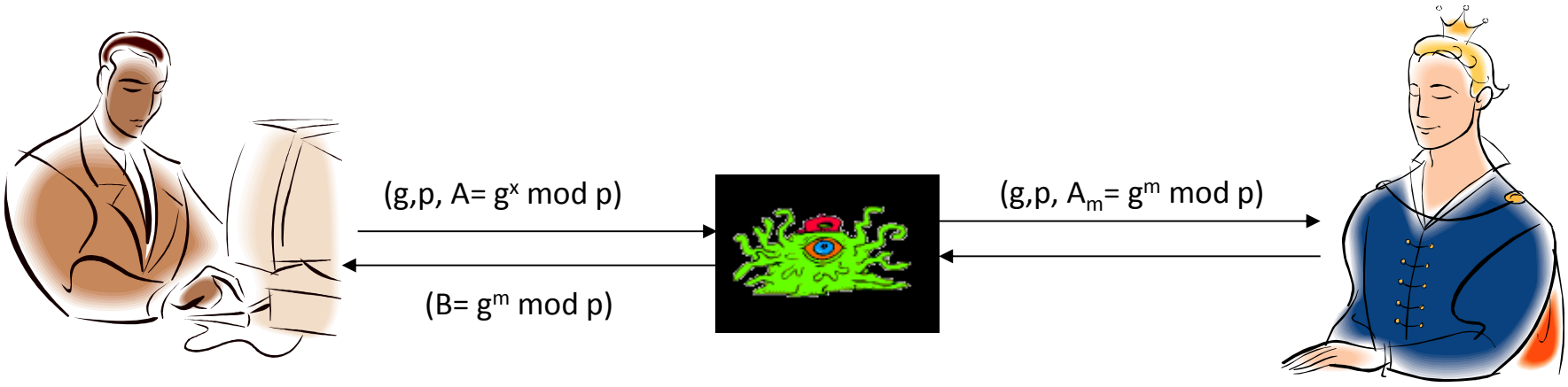
Bob

Man in the Middle

Alice

Diffie Hellman

- Man in the middle attack



Bob

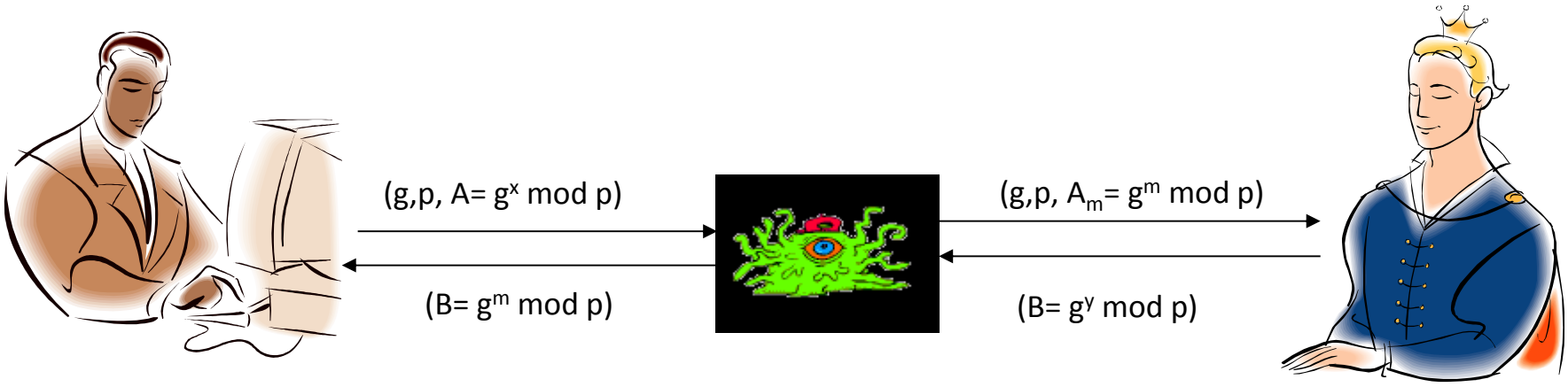
Man in the Middle

$K_{Bob} = g^{mx} \bmod p$

Alice

Diffie Hellman

- Man in the middle attack



Bob

La clés de communication avec Alice est
$K = g^{mx} \bmod p$

Man in the Middle

$K_{Bob} = g^{mx} \bmod p$

$K_{Bob} = g^{my} \bmod p$

Alice

La clés de communication avec Bob est
$K = g^{my} \bmod p$

Diffie Hellman

- Secure against eavesdroppers.
- Can be secured against man-in-the-middle by using authenticated g^b mod p or by using a published value g^b mod p.
- The problem is one of authentication and trust.

Diffie Hellman and all other schemes

- Ce protocole est un premier algorithme à clé publique limitée à l'échange de clés.
- Dépendant de son efficacité sur la difficulté de calculer un logarithme discret.
- Offre une protection contre les attaques passives.
- Peut être sécurisé contre les attaques actives?

Les algorithmes symétriques (avantages)

- Les algorithmes symétriques offrent un niveau de sécurité assez élevé tout en permettant aux messages d'être cryptés et décryptés rapidement.
- La relative simplicité des systèmes symétriques est également un avantage logistique, car ils nécessitent moins de puissance de calcul que les systèmes asymétriques.
- De plus, la sécurité fournie par le chiffrement symétrique peut être augmentée simplement en augmentant la longueur des clés. Pour chaque bit ajouté à la longueur d'une clé symétrique, la difficulté de déchiffrer le chiffrement par une attaque par force brute augmente de façon exponentielle.

Les algorithmes symétriques (inconvénient)

- Bien que le chiffrement symétrique offre un large éventail d'avantages, il présente un inconvénient majeur:
- le problème inhérent de transmission des clés utilisées pour chiffrer et déchiffrer les données. Lorsque ces clés sont partagées sur une connexion non sécurisée, elles sont susceptibles d'être interceptées par des tiers malveillants.
- Si un utilisateur non autorisé accède à une clé symétrique particulière, la sécurité de toutes les données chiffrées à l'aide de cette clé est compromise.
- Pour résoudre ce problème, de nombreux protocoles Web utilisent une combinaison de chiffrement symétrique et asymétrique pour établir des connexions sécurisées.
- Il convient également de noter que tous les types de cryptage informatique sont sujets à des vulnérabilités en raison d'une mauvaise mise en œuvre. Alors qu'une clé suffisamment longue peut rendre une attaque par force brute mathématiquement impossible, les erreurs de mise en œuvre faites par les programmeurs créent souvent des faiblesses qui ouvrent la voie aux cyberattaques.