4. Cryptographie Moderne
2. Cryptographie Asymétrique

Noureddine AZZOUZA Riadh MEGHATRIA

[1] Université Djilali BOUNAAMA Khemis Miliana, Algérie

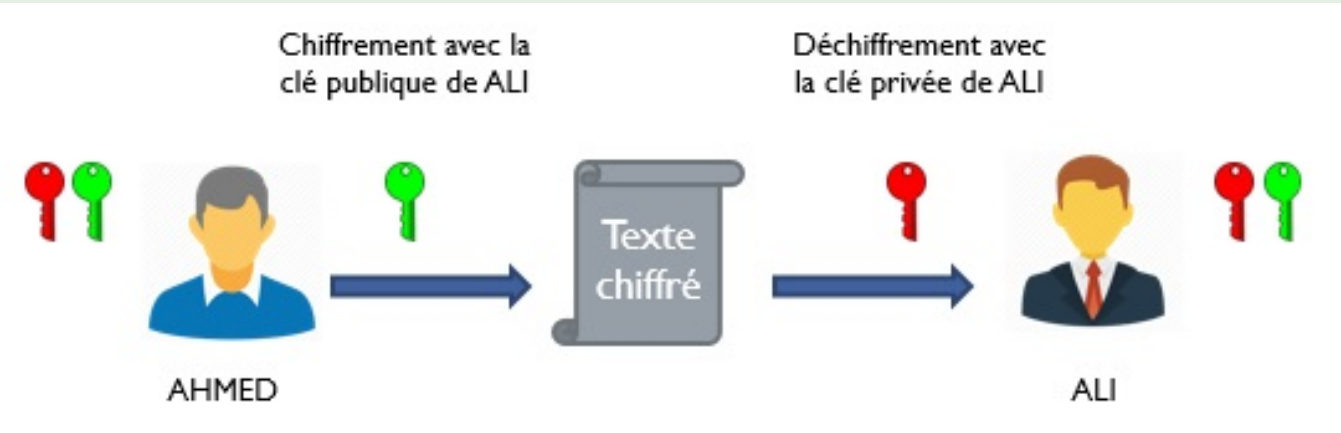
Cours de Sécurité Informatique, M2GLSD

Cryptographie asymétrique : Principe

Principe

- Une paire de clés pour chaque personne
- Une clé publique et une clé privée ou secrète.
- Clé publique différente de la clé privée
- Message chiffré avec l'une des 2 clés —> ne peut être déchiffré qu'avec la 2^{ieme} clé

Cryptographie asymétrique



Cryptographie asymétrique : Avantages et inconvénients

Principe

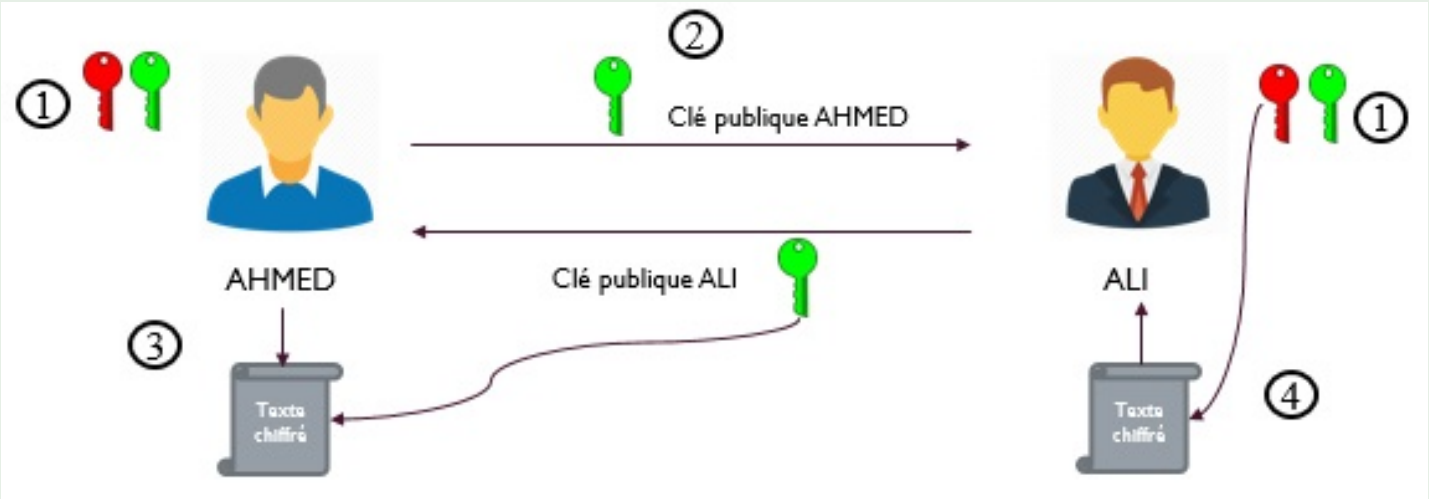
- Nombre de clés réduit
- distribution des clés simple
- Ajout d'utilisateur facile

Principe

- Lent par rapport aux algorithmes de la cryptographie symétrique
- Vulnérable à certaines attaques(Essayer de chiffrer autant de textes clairs et comparer jusqu'à trouver le bon)

Cryptographie asymétrique : Confidentialité

Confidentialité



Étapes :Confidentialité

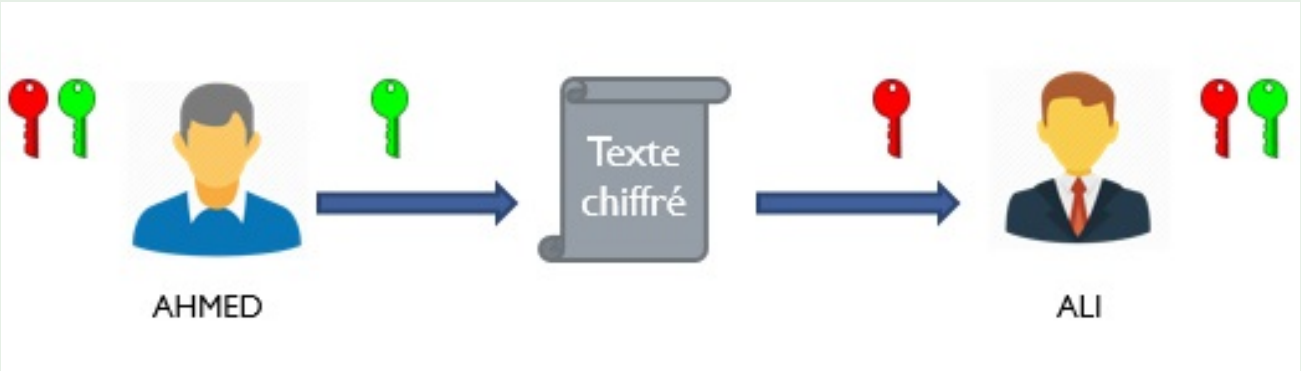
1. Création des clés (publique et privée)
2. Échange des clés publique (ou publication sur un serveur dédié)
3. AHMED chiffre un message M avec la clé publique de ALI
4. ALI déchiffre le message M avec sa clé privée (Seul ALI peut lire le message)

Cryptographie asymétrique : Authentification

Authentification

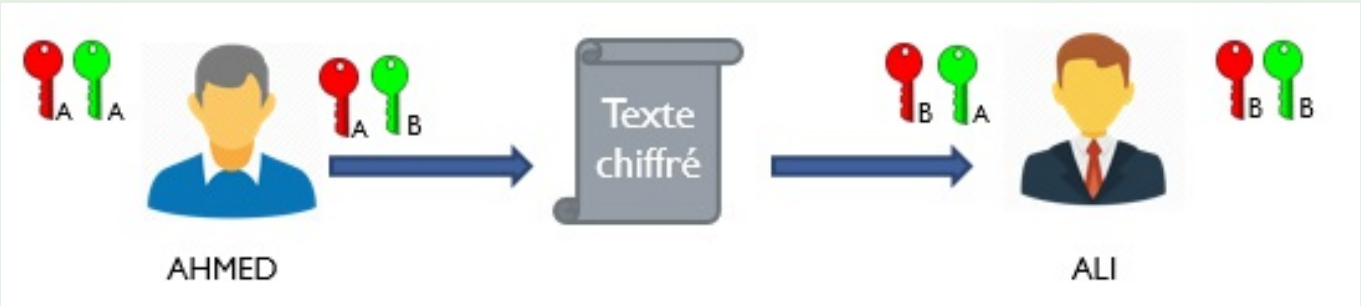
- AHMED envoie un message crypté à ALI
- ALI veut s'assurer s'il s'agit bien de AHMED
- ALI envoie un défi à AHMED (message chiffré avec la clé publique de AHMED)
- AHMED déchiffre le défi avec sa clé privée et renvoie le défi en clair à ALI
  - Preuve que AHMED possède bien la clé privée correspondante à la clé publique que ALI utilise

Authentification



Cryptographie asymétrique : Confidentialité + Authentification

Confidentialité + Authentification

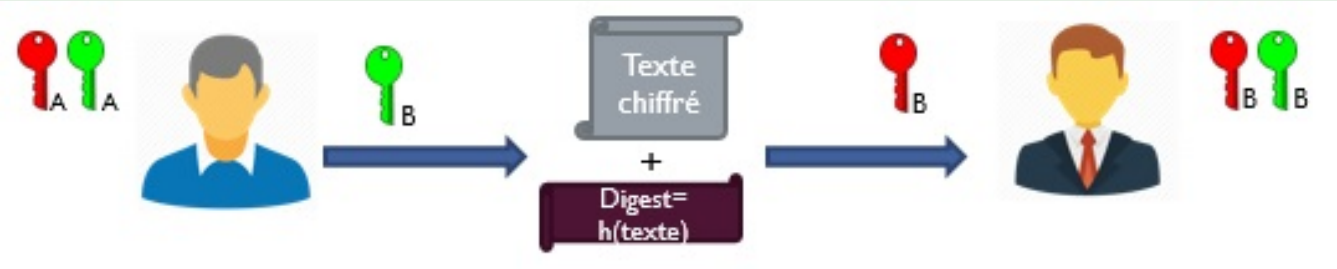


Confidentialité + Authentification

1. AHMED chiffre le message sa clé privée (authentification)
2. AHMED chiffre encore le message avec la clé publique de ALI et l'envoie (confidentialité)
3. ALI déchiffre le message avec sa clé privée
4. ALI déchiffre ensuite le message par la clé publique de AHMED (M provient certainement de AHMED

Cryptographie asymétrique : Intégrité

Intégrité



Intégrité

1. Message M –> Digest (128 à 160 bits) est un code généré par une fonction de hachage
2. Fonction de hachage : exemple (SHA 160bits, MD5 128 bits)
3. ALI reçoit le texte et son digest
4. Calcul à nouveau le digest = h(M) et compare les 2 pour vérifier l'intégrité du message

Nombres premiers

Nombres premiers

1. X est un entier positif premier si X admets 2 diviseurs distincts : 1 et lui même
2. Exemple : 2, 3, 5, 7, 11, 13, 17, 19, ?

Nombres premiers entre eux

1. p et q sont premiers entre eux si pgcd(p,q) = 1
2. Exemple : 11 et 17 sont premiers entre eux

Congruence

Congruence

- a = r (mod n)
- a - r = k * n (r est le reste de la division de a par n)
- a et b sont congrus modulo n s'ils ont même reste par la division par n
- Exemple : 13 = 6 (mod 7) = 6(7) ; 13 = 3 (mod 10) ; 21 = 1 (10)

Propriétés

Si $a = r_a$ (n) et $b = r_b$ (n)

Alors:

$a + b = r_a + r_b$ (n)

$a - b = r_a - r_b$ (n)

$a * b = r_a * r_b$ (n)

Si $a^{k-1} = r'$ (n) et $a = r$ (n)

Alors:

$a^k = rr'$ (n)

Calculer a^k → proche en proche

10^5 (mod 85)

$10^2 = 100$

$100 = 15$ (mod 85)

$10^4 = (10^2)^2$

$(10^2)^2 = 15^2 = 255$

$225 = 55$ (mod 85)

$10^5 = 10^4 \times 10$

$55 \times 10 = 550$

$550 = 40$ (mod 85)

Inverses

Inverses

1. Si ab = 1 (mod n) alors a et b sont inverses
2. Exemple
   1. 4 et 2 sont inverses modulo 7 –> 4*2 = 8 = 1(7)
   2. 5 et 3 sont inverses modulo 14 –> 5*3 = 15 = 1(14)

Equation

ax = 1 (mod n) –> trouver x l'inverse a

1. Algorithme d'Euclide étendu
2. Théorème d'Euler et Fermat généralisé

Inverses

Théorème de Fermat

1. $a^{(n-1)} = 1(n)$ si n et a sont premiers entre eux
2. Exemple : $7^{12} = 1(13)$

Fonction d'Euler

1. $n \rightarrow \varphi(n)$: nombre d'entiers < n et qui sont premiers avec n
2. Si n est premier alors : $\varphi(n) = n - 1$
3. Si n = p*q (p et q sont premiers) alors $\varphi(n) = \varphi(pq)$ = (p-1)(q-1) ;
4. Exemple
   1. N = 7 $\rightarrow \varphi(7)$ = 6 1, 2, 3, 4, 5, 6
   2. N = 15 $= 5 * 3 \rightarrow \varphi(15) = \varphi(3) * \varphi(5)$ = 2 x 4 = 8 1, 2, 4, 7, 8, 11, 8, 11, 13, 14

Théorème de Fermat généralisé

1. Si a et n sont premiers entre eux alors $a^{\varphi(n)} = 1(n)$

Inverses

Équation

1. ax = 1(n)
2. Si $a^{\varphi(n)} = 1(n)$ alors $a^{(\varphi(n)-1)} * a = 1(n)$
3. $a^{(\varphi(n)-1)}$ et a sont inverses

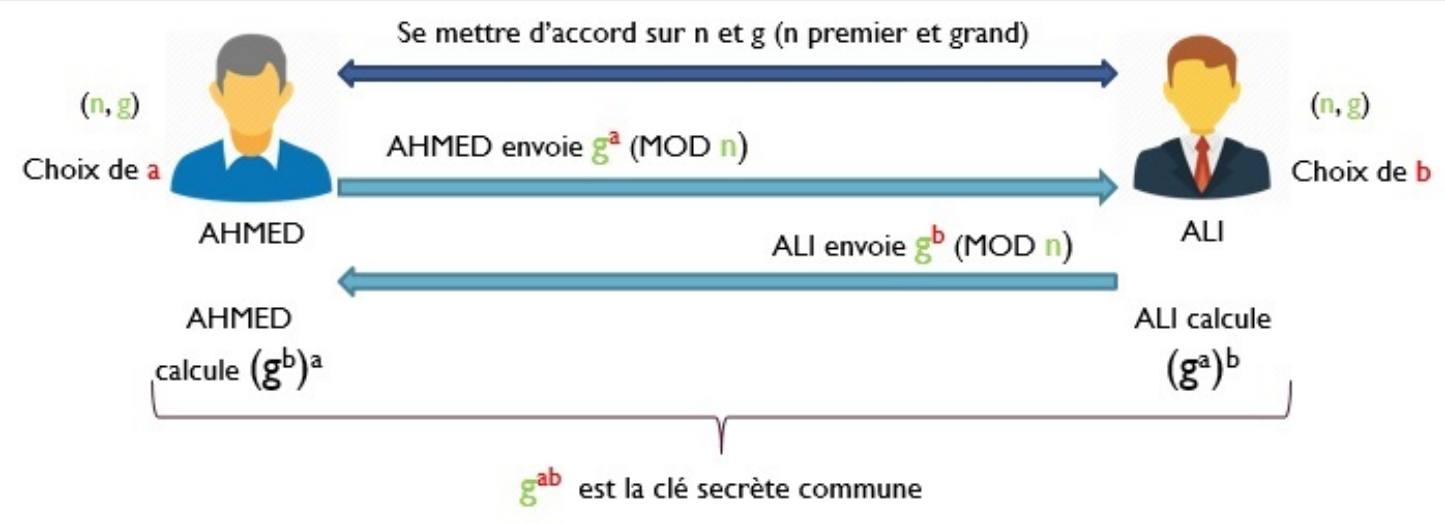
Logarithme discret

est l'inverse de celui de l'exponentiel

1. Equation : ax = b(n) $\rightarrow$ trouver x ?
   1. 5^x=3(7) $\rightarrow$ sol : x = 5
   2. 3^x=15(17) $\rightarrow$ sol : x = 6
   3. 3^x=7(13) $\rightarrow$ pas de solution

Algorithme de Diffie-Hellman

clé de session



Intégrité

1. n, g : publiques
2. a, b : privés et impossible à trouver
3. ALI reçoit le texte et son digest
4. g^{ab} : clé secrète impossible à trouver (problème de logarithme discret)

Algorithme RSA

Chiffrement par bloc

1. Ronald Rivest, Adi Shamir et Leonard Adleman MIT 1978
2. Algorithme très utilisé
3. emploie de grands nombres entiers (par exemple 1024 bits)
4. Basé sur :
   1. Arithmétique modulaire
   2. Factorisation des nombres

Algorithme RSA : Vue globale

Principe

- Clé publique k : k = (e, n) 2 entiers premiers
- Chiffrement E : $E_k(M) = M^e(mod n) = C$
- Clé privée k' : k' = (d, n)
- Déchiffrement D : $D_{k'}(C) = C^d(mod n) = M$

Exemple

1. n = 23 ; e = 9 ; d = 5
2. (M = 2) $\rightarrow 2^9 = 512 = 6$ (23) et $6^5 = 2$(23) (C = 6)
3. (M = 2) $\rightarrow 2^5 = 32 = 9$ (23) et $9^9 = 2$(23) (C = 9)

Algorithme RSA : Préparation des clés

Principe

1. choix des deux nombres premiers
   - AHMED choisit 2 nombres premiers distincts p et q
   - Calcul $n = pxq$
   - Calcul $\varphi(n) = (p-1) \times (q-1)$

Exemple

1. p = 5 et q = 17
2. $n = p \times q$ = 85
3. $\varphi(n) = (p-1) \times (q-1)$ = 4 x 16 = 64

Algorithme RSA : Préparation des clés

Principe

2. Choix d'un exposant et calcul de son inverse
   - AHMED choisit un exposant e tel que $pgcd(e, \varphi(n)) = 1$
   - AHMED calcule l'inverse d de e modulo $\varphi(n)$ par l'algorithme d'Euclide étendu : $d \times e = 1 (mod \varphi(n))$

Exemple

1. e = 5 et on a bien $pgcd(e, \varphi(n)) = pgcd(5, 64) = 1$
2. $5 \times 13 + 64 \times (-1) = 1$
3. Donc $5 \times 13 = 1 \pmod{64}$
4. L'inverse de e modulo $\varphi(n)$ est d = 13

Algorithme RSA : Préparation des clés

Principe

3. clé publique
   - La clé publique d'AHMED est constituée de 2 nombres : n et e
4. clé privée
   - AHMED grade pour elle sa clé privée : d et n qu'il connait déjà
5. AHMED peut maintenant détruire les nombre p , q et $\varphi(n)$

Exemple

1. n = 85
2. e = 5
3. d = 13

Algorithme RSA : Chiffrement

Chiffrement

1. ALI veut envoyer un message secret à AHMED
2. Il transforme son message en un (ou plusieurs) entier : avec $0 < m < n$
3. ALI récupère la clé publique d'AHMED : n et e
4. Il calcule le message chiffré $x = m^e \pmod n$
5. ALI transmet ce message x à AHMED

Exemple

1. $m = 10$; $n = 85$; $e = 5$
2. $x = m^e \pmod n = 105 \pmod{85}$
   - $10^2 = 100 = 15 \pmod{85}$
   - $10^4 = (10^2)^2 = 15^2 = 225 = 55 \pmod{85}$
   - $10^5 = 10^4 \times 10 = 55 \times 10 = 550 = 40 \pmod{85}$

Algorithme RSA : Déchiffrement

Déchiffrement

1. AHMED reçoit le message x chiffré par ALI
2. Il le déchiffre à l'aide de sa clé privée d
3. m = x^d (mod n)

Exemple

1. x = 40 ; d = 13 ; n = 85
2. x = m^e(mod n) = 105 (mod 85)
   - $40^2 = 1600 = 70 \pmod{85}$
   - $40^4 = (40^2)^2 = 70^2 = 4900 = 55 \pmod{85}$
   - $40^8 = (40^4)^2 = 55^2 = 3025 = 50 \pmod{85}$
   - $40^13 = 40^{8+4+1} = 40^8 \times 40^4 \times 40 = 50 \times 55 \times 40 = 10 \pmod{85}$
3. m = 10