# Chiffrement Asymétrique

Dr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

# Plan du cours

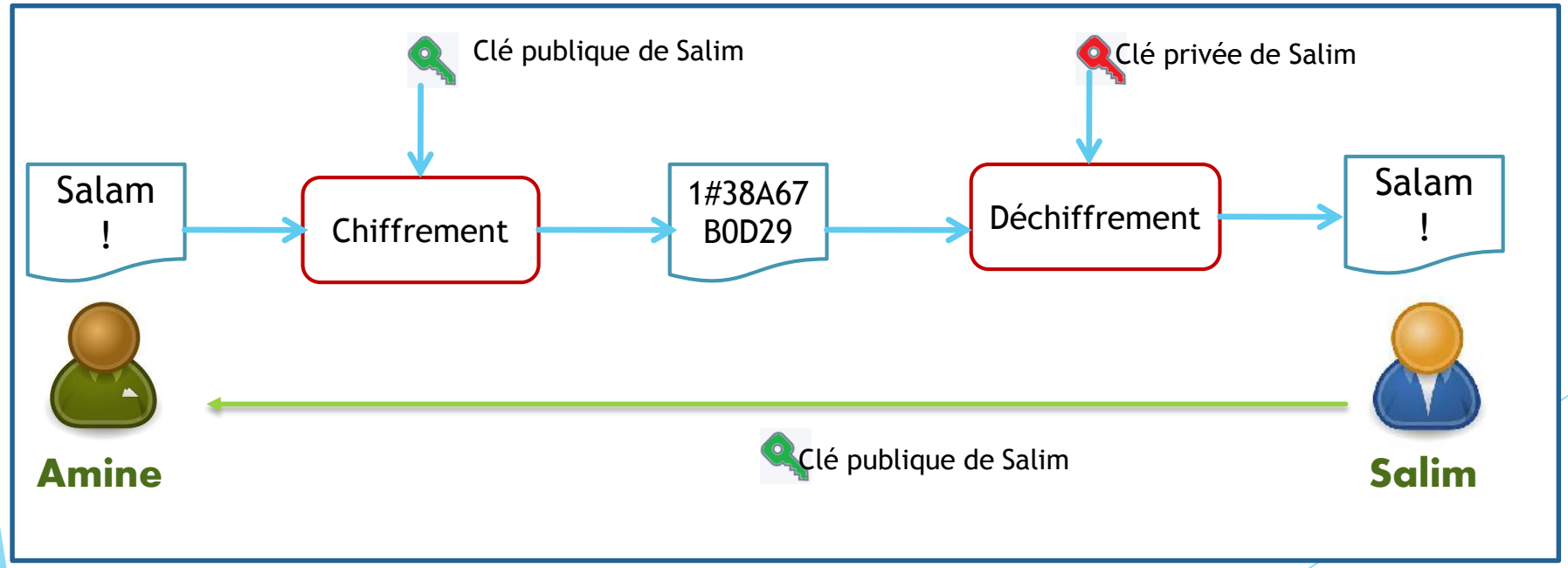
- Principes
- Concepts mathématiques
- Cryptosystème RSA

# Cryptographie asymétrique: Principes

- également appelée, cryptographie à clé publique (PKC en anglais pour Public Key Cryptography).
- sa sécurité repose sur la difficulté des problèmes computationnels.

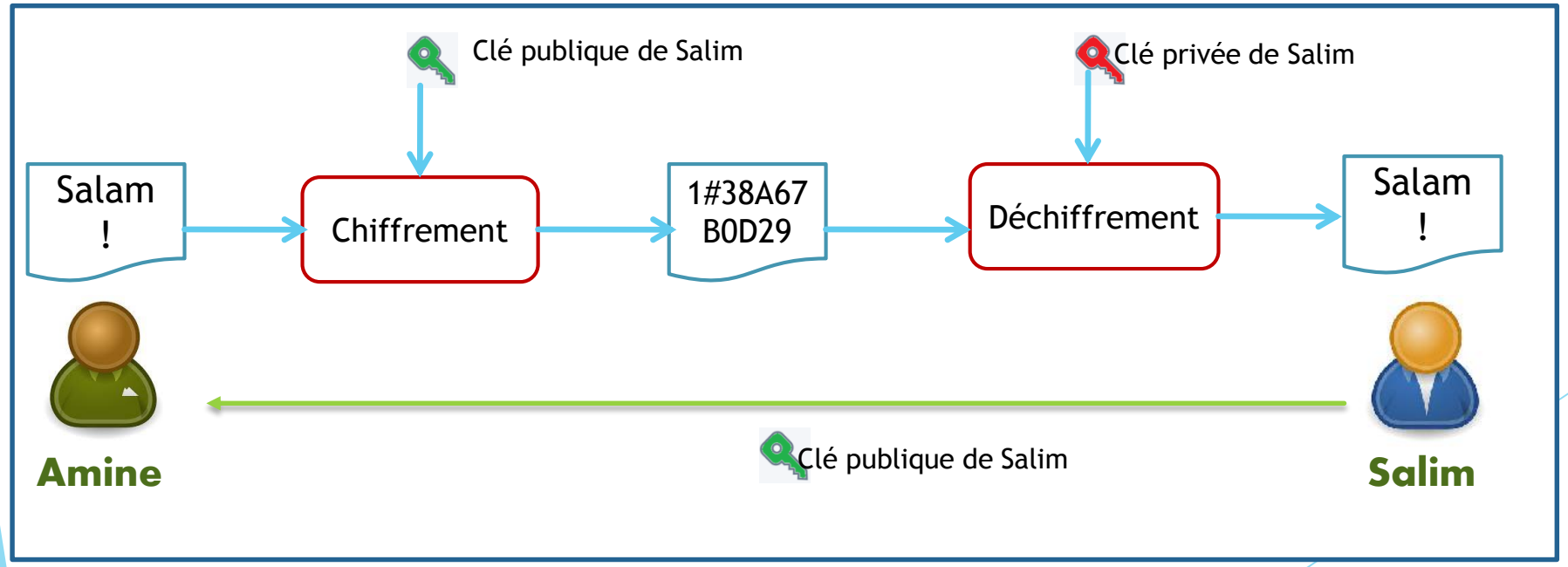
# Cryptographie asymétrique: Principes

- Chaque entité possède une paire des clés (clé publique, clé privée).
- Les deux clés sont liées mathématiquement.
- La clé publique est connu pour tout le monde.
- Pour chiffrer un message, on utilise la clé publique de destinataire.



# Cryptographie asymétrique: Principes

- La clé privée ne circule jamais sur le réseau,
- La clé privée utilisée pour déchiffrer le message chiffré reçu.



# Cryptographie asymétrique: principes

- Les algorithme cryptographiques asymétriques sont utilisés, par exemple:
- Fournir des services d'authentification de la source, de l'identité et de l'intégrité à l'aide des signatures numériques;
- Par les protocoles d'échange de clés.
- Par les infrastructures à clés publiques.
- Pour protéger la confidentialité des données.

# Concepts mathématiques
# Les nombres premiers

## Les nombres premiers:

- Un entier naturel *p* est dit premier si il n'admet comme diviseur que 1 et lui-même.
- Les autres nombres sont dits composés. (0 et 1 sont exclus).

# Concepts mathématiques
# Les nombres premiers

## Décomposition en facteur irréductibles.

- Théorème: Tout nombre entier supérieur à 1 peut se décomposer comme un produit unique de nombres premiers.

$$a = \prod_{i=1}^{k} p_i^{n_i} = p_1^{n1} p_2^{n2} \ldots p_k^{nk}$$

- Cette écriture est appelée la décomposition de $a$ en facteur irréductibles.
- Exemple: $12348 = 2^2 * 3^2 * 7^3$

# Concepts mathématiques
# Test de primalité

## Test de primalité

- 2019 est- il premier ? Il faut tester la possibilité de division 2019/n pour:
  - Algo 1: pour tout n entier entre 2 et 2019-1
  - Algo 2: pour tout n entier entre 2 et $\sqrt{2019}$
  - Algo 3: (Crible d'Eratostene) pour tout n premier entre 2 et $\sqrt{2019}$

# Concepts mathématiques
# Test de primalité

## Théorème de Fermat:

- Soit p un nombre premier.
- Pour tout entier naturel a premier avec p , on a:

$$a^{p-1} = 1 \bmod p.$$

# Concepts mathématiques
# Test de primalité

## Test de Fermat:

- C’est une méthode probabiliste pour tester la primalité d’un entier.
- On choisit au hasard un nombre a tel que $1<a\leqslant p-1$
  - Si $a^{p-1} = 1 \bmod p$, on dit que p est pseudo(-Fermat)-premier à base a.
  - Si $a^{p-1} \neq 1 \bmod p$, alors p n'est pas un nombre premier.

# Concepts mathématiques
# Test de primalité

## Test de Fermat:

- Exemple: p = 341 = 11 * 31 (est un nombre composé)
- a=2: $2^{340} = 1 \pmod{341}$
- a=3: $3^{340} = 56 \pmod{341}$
- Donc, le test de Fermat, avec p=341 et a=3, prouver que p est composé.

# Concepts mathématiques
# Test de primalité

Autres algorithmes de test de primalité:

- Test de Miller-Rabin
- Critére de Lucas
- ….

# Concepts mathématiques
# L'indicatrice d'Euler

- Soit *n* est un entier plus grand que 2,
- l'indicatrice d'Euler de n, noté $\varphi(n)$, désigne le nombre d'entiers compris entre 1 et n, et premiers avec n.
- Si n est premier, $\varphi(n) = n - 1$.
- Si n = pq, tels que p et q sont des nombres premiers, $\varphi(n) = \varphi(p)\ \varphi(q) = (p-1)(q-1)$.
- $\varphi(p^k) = p^{k-1}(p-1)$

# Concepts mathématiques
# L'indicatrice d'Euler

## Exemples:

- $\varphi(11) = 11 - 1 = 10$
- $\varphi(15) = (5-1)(3-1) = 8$

## Théorème d'Euler:

- Pour tout entier *n* et tout *a* ∈ Z, on a:

$$a^{\varphi(n)} = 1 \bmod n$$

# Concepts mathématiques
# Fonction à sens unique

- Les problèmes computationnels utilisés dans la cryptographie à clé publique fondés sur l'existence de **fonctions à sens unique.**
- On suppose $F(x) = y$ une fonction à sens unique.
  - $F$ facile à calculer: Il est facile (temps polynomial) de calculer $F(x)$ pour importe quel $x$.
  - $F$ difficile à inverser: Il est difficile pour $y \in F$ de trouver un $x$ tel que $F(x) = y$.

# Concepts mathématiques
# Factorisation des nombres

- Factorisation des entiers:
  - Soient deux grands nombre premiers, $p$ et $q$.
  - Calculer $p \times q$ est plus facile.
  - Problème: Factoriser $n = pq$.
  - **Applications:** cryptosystèmes: RSA, Rabin.

# Concepts mathématiques
# Factorisation des nombres

Test (concours)

- Trouver les deux facteurs premiers des produits suivants:
- 35
  - 5 × 7
- 221
  - 13 × 17
- 4453
  - 61 × 73
- 503807
  - 521 × 967
- 50123093
  - 7297 × 6869

# Concepts mathématiques
# Factorisation des nombres

- Trouver les deux facteurs premiers du produit suivant:

310741824049004372135075003588856793003734602284272754572016194882320644051808150455634682967172328678243791627283803341547107310850191954852900733772482278352574238645401469173660247765234660 9

=1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579

×1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

- Les clés RSA sont habituellement d'une taille comprise entre 1024 (309 chiffres) et 2048 bits (617 chiffres).
- En décembre 2018, le plus grand nombre premier est $M_{82589933}=2^{82589933}-1$ (*nombres de Mersenne*) comportant 24 862 048 chiffres lorsqu'il est écrit en base 10.

# Concepts mathématiques
# Exponentiation modulaire

- Il existe de nombreuses algorithmes de test de primalité d'un nombre ou des algorithmes cryptographiques utilisent le calcul de l'exponentiation modulaire de façon de puissances $a^e \pmod{n}$ pour de grandes valeurs de l'exposant *e*.
- On présente une méthode considérée comme standard pour effectuer une exponentiation modulaire. Elle utilise le principe *d'élever au carré et multiplier*.

# Concepts mathématiques
# Exponentiation modulaire

- Cette technique repose sur l'écriture de l'exposant *e* en numération binaire.
- Soit e=29 = $(11101)_{2.}$
- On a *e*= 16 + 8 + 4 + 1 et $a^e = a^{16}*a^8*a^4*a$

# Concepts mathématiques
## Exponentiation modulaire

Input : a ,n, e avec e = $(e_{m-1}, .., e_0)_2$

Output : r = $a^e$ (mod n)

Begin

r ← $a^{e_{m-1}}$

for i ← m − 2 to 0 do

r ← r*r mod p

if $e_i$ = 1 then r ← r* a mod p

end for

end

# Concepts mathématiques
## Exponentiation modulaire

- Exemple:
- $15^{29} \bmod 101 = ?$
- $29 = (11101)_2$ , la taille de la suite binaire, m=5

| i | - | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|
| ei | 1 | 1 | 1 | 0 | 1 |
| r | 15 | 23 | 47 | 4 | 16 |
| r=r*y | - | 42 | 99 | - | 38 |

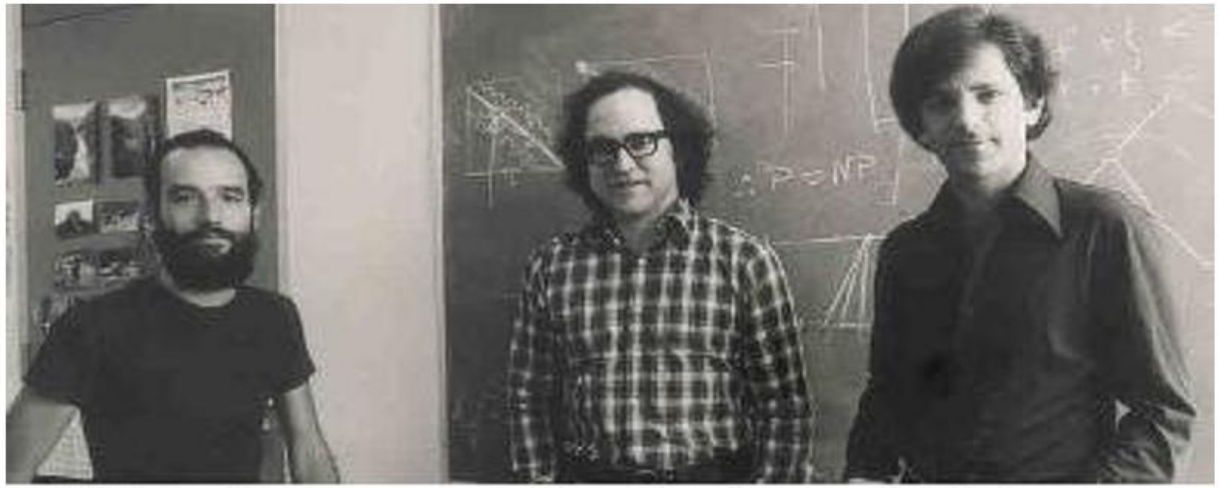
- $15^{29} \bmod 101 = 38$

# Plan du cours

- Principes
- Concepts mathématiques
- Cryptosystème RSA

# Cryptosystème RSA

- inventé en 1977 par:




- La sécurité fournie par RSA repose sur la difficulté à factoriser de grands entiers.

# Cryptosystème RSA

- Serveurs Web, Cartes de crédit, Internet (SSL/TLS), paiement électronique, …
- Microsoft,  Apple Computer, Cisco Systems, Intel, …

# RSA: Génération des clés

***Module RSA:***

- p et q sont deux nombres premiers secrets de même taille.
- N = p.q est le module RSA.

***L'indicateur d'Euler:***

- $\Phi$(N) = (p - 1)(q - 1).

***Les clés:***

- Choisir e: un entier premier, 1≤ e ≤ $\varphi(N)$ , PGCD(e, $\varphi(N)$)=1
- Calculer d, tel que: 1 ≤ d ≤ $\varphi(N)$, e.d ≡1 (mod $\varphi(N)$)

  → d = $e^{-1}$ mod $\varphi(N)$

- Clé publique: e, n
- Clé privée: d

# RSA: Chiffrement & Déchiffrement

***B veut envoyer un message à A:***

1) A génère les clés (e,d) et publie la clé publique (e,N)
2) Chiffrement: B calcule $c \equiv m^e \pmod N$ et envoi c à A.
3) Déchiffrement: A calcule $c^d \equiv m \pmod N$ et retrouve le message *m* de B.

# Cryptosystème RSA: Exemple

- A génère les clés:
- p = 11 et q= 5
- N= p*q = **55**
- $\varphi(55)$ = (11-1)*(5-1) = **40**
- A Choisit e:
  - **e** est premier
  - Soit e=3 (par exemple, et on a bien ($e$, $\varphi(55)$)=1)
- A calcule d:
  - **e.d** ≡1 (mod 40) → d = $3^{-1}$ mod 40
  - On détermine que d=27 (inverse modulaire de $e$ sur $Z_{\Phi(n)}$)

Clé publique **(55,3)** et la clé privée **(27)**

# Cryptosystème RSA: Exemple

- B veut envoyer un message (m=51) à A:
  - B calcule c= $51^3$ mod 55 = 46
  - B envoie c= 46 à A.
- A reçu le message:
  - A calcule m= $46^{27}$ mod 55 = 51

# Recommandation pour l’utilisation du RSA

- Utilisation des clés fortes, p et q ont des grandes nombres premiers.
- La taille du texte à chiffrer est importante,
- N’utilise pas un module RSA n commun à plusieurs clés.

# Factorisation du module RSA

- Le module RSA-250 a une taille de 829 bits , équivalant 250 chiffres décimaux.
- RSA-250 a été factorisé le 28 février 2020 par F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé et P. Zimmermann.
- Cette factorisation a été trouvée en utilisant l'algorithme Number Field Sieve en utilisant l'application open-source CADO-NFS.

# Recommandation

- NIST (2019)

| Date | Niveau de Sécurité | Algorithme symétrique | Factorisation Module | Logarithme discret Clef | Logarithme discret Groupe | Courbe elliptique | Hash (A) | Hash (B) |
|---|---|---|---|---|---|---|---|---|
| Legacy [1] | 80 | 2TDEA | 1024 | 160 | 1024 | 160 | SHA-1 [2] | |
| 2019 - 2030 | 112 | (3TDEA) [3] AES-128 | 2048 | 224 | 2048 | 224 | SHA-224 SHA-512/224 SHA3-224 | |
| 2019 - 2030 et au-delà | 128 | AES-128 | 3072 | 256 | 3072 | 256 | SHA-256 SHA-512/256 SHA3-256 | SHA-1 KMAC128 |
| 2019 - 2030 et au-delà | 192 | AES-192 | 7680 | 384 | 7680 | 384 | SHA-384 SHA3-384 | SHA-224 SHA-512/224 SHA3-224 |
| 2019 - 2030 et au-delà | 256 | AES-256 | 15360 | 512 | 15360 | 512 | SHA-512 SHA3-512 | SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256 |

https://www.keylength.com/fr/4/

# Autres Algorithmes

- Cryptosystème **El Gamal**, inventé en 1984

- La sécurité de ce cryptosystème basée sur le problème du logarithme discret.

# Autres Algorithmes

- **ECC (Elliptic Curve Cryptography),** inventé en 1985 par Koblitz et Mille

- La sécurité de ce crypto-système basée sur le problème du ***logarithme discret elliptique***.

# Exercice

Soient n = 85 et e= 7 (clé publique).

- Trouver p et q
- Calculer $\Phi$(n) et d.
- Chiffrer le message m = 12