

Asymmetric Encryption

Pr. Nouredine Chikouche

[nouredine.chikouche\[@\]univ-msila.dz](mailto:nouredine.chikouche[@]univ-msila.dz)

<https://sites.google.com/view/chikouchenouredine>

Course outline

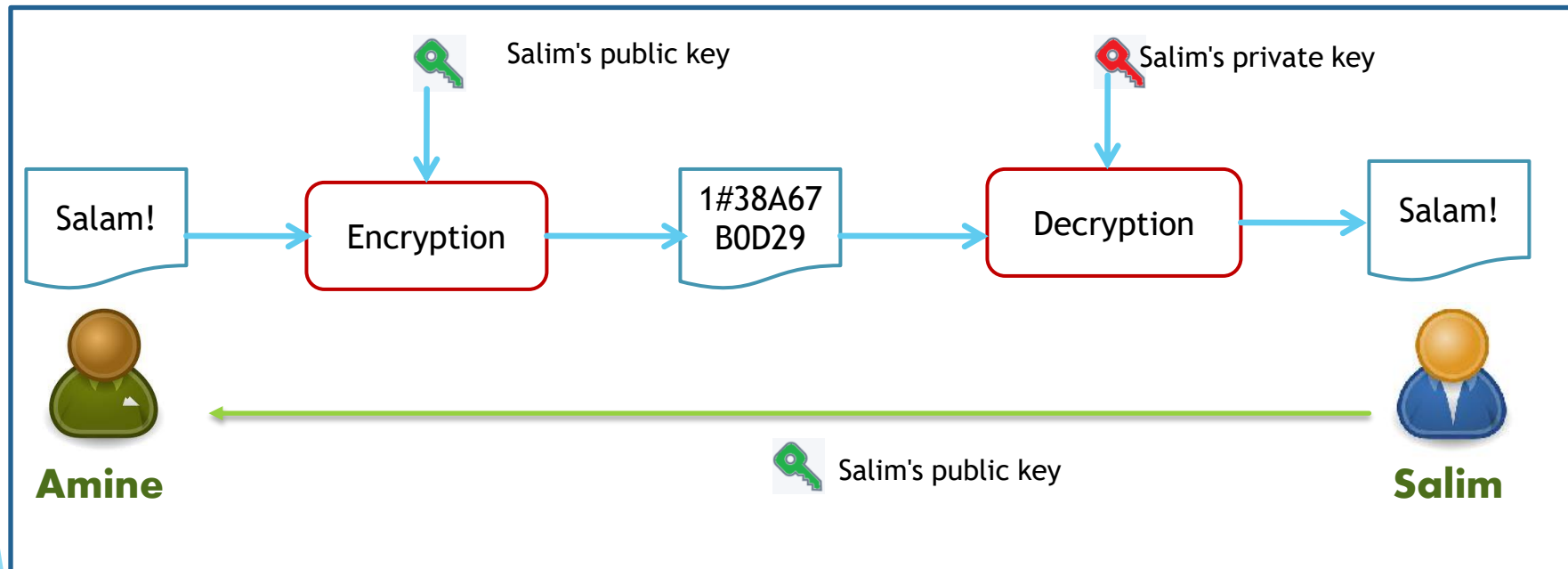
- Principles
- Mathematical concepts
- RSA Cryptosystem

Asymmetric cryptography: Principles

- Also called: public key cryptography (PKC stands for Public Key Cryptography).
- The security of PKC based on **difficulty of computational problems**.

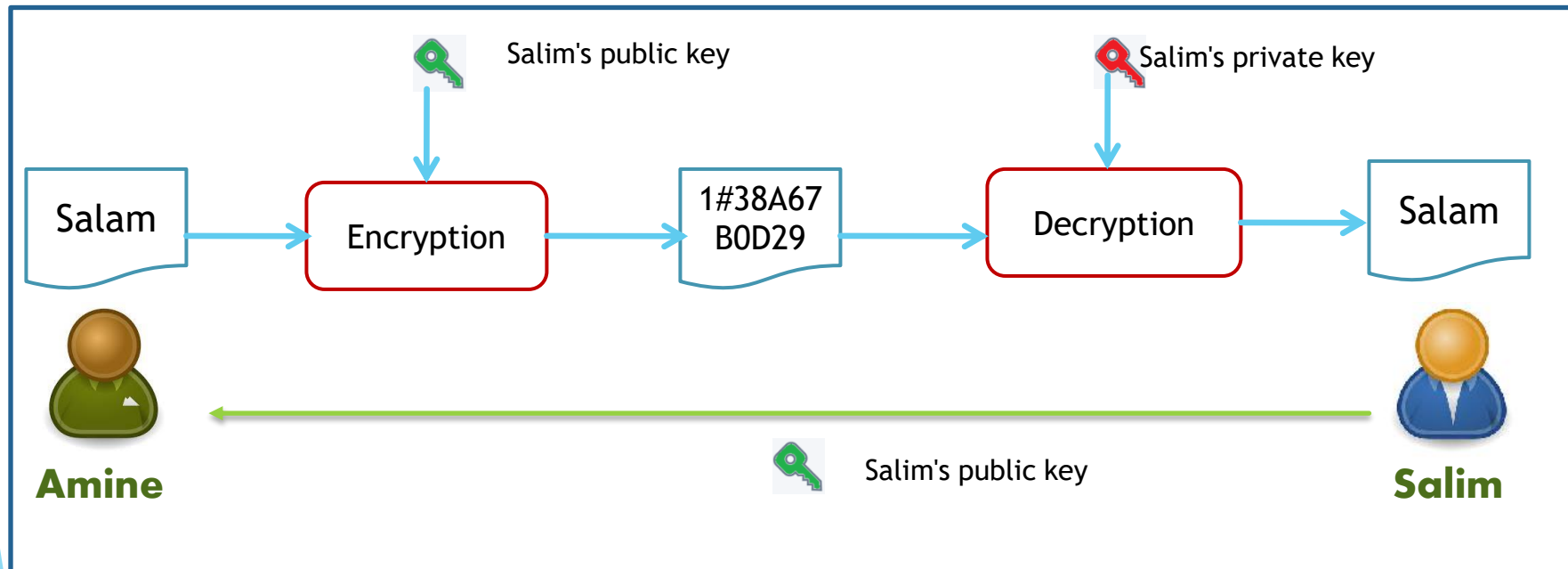
Asymmetric cryptography: Principles

- Each entity has a key pair (public key, private key).
- The two keys are linked **mathematically**.
- The public key is known to everyone.
- To encrypt a message, we use the recipient's public key.



Asymmetric cryptography: Principles

- The private key never transmitted over the network.
- The private key used to decrypt the ciphertext.



Mathematical concepts

Trapdoor one-way function

- ▶ The computational problems used in public-key cryptography are based on the existence of **trapdoor one-way function**.
- ▶ We assume $F(x) = y$ as one-way function.
 - ▶ **F is easy to calculate:** It is easy (polynomial time) to calculate $F(x)$ for any x .
 - ▶ **F is difficult to reverse:** It is difficult for $y \in F$ to find a x such as $F(x) = y$.
- ▶ In the function **with trapdoor**: Calculating the inverse will be easy if we know a **additional information**. The trapdoor is the *key private of the recipient*.

Asymmetric Cryptography: principles

- ▶ The asymmetric cryptography algorithms are used, for example:
 - ▶ Provide source authentication services, identity, and integrity using digital signatures;
 - ▶ Exchange keys protocols.
 - ▶ Public key infrastructures.
 - ▶ To protect data confidentiality.

Mathematical concepts

Prime numbers

Prime Numbers:

- ▶ A natural number p is said to be **prime** if its only divisors are 1 and itself.
- ▶ All other numbers are called **composite** numbers.
(0 and 1 are excluded).

Mathematical concepts

Prime numbers

Decomposition into irreducible factors.

- ▶ **Theorem:** Any integer greater than 1 can be decomposed as a single product of prime numbers.

$$a = \prod_{i=1}^k p_i^{n_i} = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

- ▶ This writing is called the decomposition of a in irreducible factors.
- ▶ Example: $12348 = 2^2 \cdot 3^2 \cdot 7^3$

Mathematical concepts

Primality Test

Primality Test

- ▶ **Is 2019 prime number?** We need to test the possibility of dividing $2019/n$ for :
 - ▶ **Algo 1:** for any integer n between 2 and $2019-1$
 - ▶ **Algo2:** for any integer n between 2 and $\sqrt{2019}$
 - ▶ **Algo3:** (**Sieve of Eratosten**) for any prime n between 2 and $\sqrt{2019}$

Mathematical concepts

Primality Test

Fermat Theorem :

- ▶ Let p is a prime number.
- ▶ For any natural number a coprime to p , we have::

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

Mathematical concepts

Primality Test

Fermat's test:

- ▶ It's a method **probabilistic** to test the primality of an integer.
- ▶ We randomly chooses a number **a** such that $1 < a \leq p-1$
 - ▶ If $a^{p-1} = 1 \bmod p$, we said that **p** is pseudo(-Fermat)-prime based **a**.
 - ▶ If $a^{p-1} \neq 1 \bmod p$, then **p** is not a prime number.

Mathematical concepts

Primality Test

Fermat's Test:

- ▶ **Example:** $p = 341$
- ▶ $a=2$: $2^{340} = 1 \pmod{341}$
- ▶ $a=3$: $3^{340} = 56 \pmod{341}$
- ▶ Therefore, Fermat's test, with $p=341$ and $a=3$, proves that p is **compound**.
- ▶ We have $341 = 11 * 31$

Mathematical concepts

Primality Test

There are several primality testing algorithms:

- ▶ Miller-Rabin test
- ▶ CriteriaLucas
- ▶ ...

Mathematical concepts

Euler's indicator

- ▶ Let n is an integer greater than 2,
- ▶ the Euler function of n , denoted $\varphi(n)$, refers **the number of intgeres between 1 and n , and prime with n .**
- ▶ If n is prime, $\varphi(n) = n - 1$.
- ▶ If $n = pq$ such that p and q are prime numbers, $\varphi(n) = \varphi(p) \varphi(q) = (p - 1)(q - 1)$.
- ▶ $\varphi(p^k) = p^{k-1}(p-1)$

Mathematical concepts

Euler's indicator

Examples:

- ▶ $\varphi(11) = 11 - 1 = 10$
- ▶ $\varphi(15) = \varphi(5) \times \varphi(3) = (5 - 1)(3 - 1) = 8$
- ▶ $\varphi(8) = \varphi(2^3) = 2^{3-1}(2-1) = 4$

Euler Theorem:

- ▶ For any integer n and everything $a \in \mathbb{Z}$, we have :

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

Mathematical concepts

Factoring numbers

- ▶ Factoring integers:
 - ▶ Let two large prime numbers, p and q .
 - ▶ Calculate $p \times q$ is easier.
 - ▶ Problem: Factorizing $n = pq$.
 - ▶ Applications: RSA and Rabin cryptosystems.

Mathematical concepts

Factoring numbers

Test (competition)

▶ Find the two prime factors of the following products:

▶ **35**

▶ 5×7

▶ **221**

▶ 13×17

▶ **4453**

▶ 61×73

▶ **503807**

▶ 521×967

▶ **50123093**

▶ 7297×6869

Mathematical concepts

Factoring numbers

- ▶ Find the two prime factors of the following product:

310741824049004372135075003588856793003734602284272754572016194882320644051808
150455634682967172328678243791627283803341547107310850191954852900733772482278
3525742386454014691736602477652346609

=1634733645809253848443133883865090859841783670033092312181110852389333100104
508151212118167511579

×1900871281664822113126851573935413975471896789968515493666638539088027103802
104498957191261465571

- ▶ RSA keys are typically between 1024 bits (309 digits) and 2048 bits (617 digits) in size.
- ▶ In December 2018, the largest prime number was $M_{82589933}=2^{82589933}-1$ (Mersenne numbers), which has 24,862,048 digits when written in base 10.

Mathematical Concepts

Modular Exponentiation

- ▶ Many primality testing algorithms and cryptographic algorithms use modular exponentiation in the form of powers $a^e \pmod n$ for large values of the exponent e .
- ▶ We present a method considered standard for performing modular exponentiation. It uses the principle of **squaring and multiplying**.

Mathematical Concepts

Modular Expansion

- ▶ This technique is based on the writing of the exponent e in numeration binary.
- ▶ Let $e=29 = (11101)_2$.
- ▶ We have $a^{e=16+8+4+1}$ and $a^e = a^{16} * a^8 * a^4 * a$

Mathematical Concepts

Modular Expansion

Input: a, n, e with $e = (e_{m-1}, \dots, e_0)_2$

Output: $r = a^e \pmod n$

Begin

$r \leftarrow a^{e_{m-1}}$

for $i \leftarrow m-2$ to 0 do

$r \leftarrow r^2 \pmod n$

If $e_i = 1$ then $r \leftarrow r \cdot a \pmod n$

endfor

end

Mathematical Concepts

Modular Expansion

- ▶ Example:
- ▶ $15^{29} \bmod 101 = ?$
- ▶ $a=15, e=29, n=101$
- ▶ $29 = (11101)_2$, the size of the binary sequence, $m=5$

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

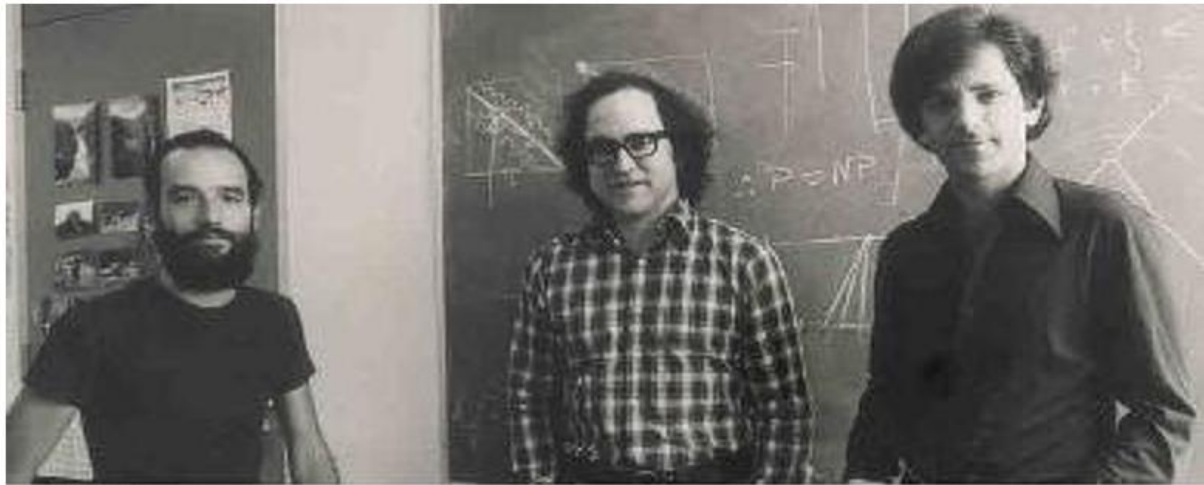
- ▶ $15^{29} \bmod 101 = 38$

Course outline

- Principles
- Mathematical concepts
- **RSA Cryptosystem**

RSA Cryptosystem

- ▶ invented in 1977 by:



Adi Shamir

Ron Rivest

Len Adleman

RSA Cryptosystem

- ▶ The security of RSA relies on the difficulty in **factoring large integers**.
- ▶ Web Servers, creditcards, Internet (SSL/TLS), e-payment, ...
- ▶ Microsoft, Apple Computer, Cisco Systems, Intel, ...

RSA: Key Generation

RSA Module:

- ▶ p and q are two secret prime numbers of the same size.
- ▶ $N=pq$ is the RSA module.

The indicator Euler:

- ▶ $\phi(N) = (p - 1)(q - 1)$.

The keys:

- ▶ Choose e : a prime integer, $1 \leq e \leq \phi(N)$, $\text{GCD}(e, \phi(N))=1$
- ▶ Calculate d , such as: $1 \leq d \leq \phi(N)$, $ed \equiv 1 \pmod{\phi(N)}$
 $\rightarrow d = e^{-1} \pmod{\phi(N)}$
- ▶ **Public key:** e, n
- ▶ **Private key:** d

RSA: Encryption & Decryption

B wants to send a message to A:

- 1) A generates the keys (e, d) and publishes the public key.
- 2) **Encryption:** B calculates $c \equiv m^e \pmod{N}$ and sending it to A.
- 3) **Decryption:** A calculates $c^d \equiv m \pmod{N}$ and retrieves the message m .

RSA Cryptosystem: Example

- ▶ A generates the keys:
- ▶ $p = 11$ and $q = 5$
- ▶ $N = p \cdot q = 55$
- ▶ $\varphi(55) = (11-1) \cdot (5-1) = 40$
- ▶ A Choisit e :
 - ▶ e is prime number.
 - ▶ Let $e=3$ (for example, and we have $(e, \varphi(55))=1$)
- ▶ Calculate d :
 - ▶ $ed \equiv 1 \pmod{40} \rightarrow d = 3^{-1} \pmod{40}$
 - ▶ We determine $d=27$ (modular inverse of e on $Z_{\varphi(n)}$)

Public Key (55.3) and the private key(27)

RSA Cryptosystem: Example

▶ B want to send a message ($m=51$) to A:

▶ B calculates $c = 51^3 \bmod 55 = 46$

▶ B sends $c= 46$ to A.

▶ Decrypting the ciphertext:

▶ Calculate $m = 46^{27} \bmod 55 = 51$

Recommendation for RSA

- ▶ Using strong keys, p and q have large prime numbers.
- ▶ The size of the text to be encrypted is important.
- ▶ Do not use a common module $RSA(n)$ with multiple keys.

Factoring of the RSA module

- ▶ The module **RSA-250** has a size of 829 bits, equivalent to 250 decimal digits.
- ▶ RSA-250 has been factored in **2020** by F.Boudot, P. Gaudry, A. Guillevic, N.Heninger, E.Thoméand P. Zimmermann.
- ▶ This factorization was found using the **Number Field Sieve** algorithm using the open-source applicationCADO-NFS.

Recommendation

► 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/>

Other Algorithms

- ▶ El Gamal cryptosystem invented in 1984



- ▶ The security of this cryptosystem based on the problem of **discrete logarithm**.

Other Algorithms

- ▶ **ECC (Elliptic Curve Cryptography)**, invented in 1985 by Koblitz and Mille.



- ▶ The security of this cryptosystem based on the problem of *discrete elliptic logarithm*.

Exercise

Let $n = 85$ and $e = 7$ (public key).

- ▶ Find p and q
- ▶ Calculate $\Phi(n)$ and d .
- ▶ Encrypt the message $m = 12$