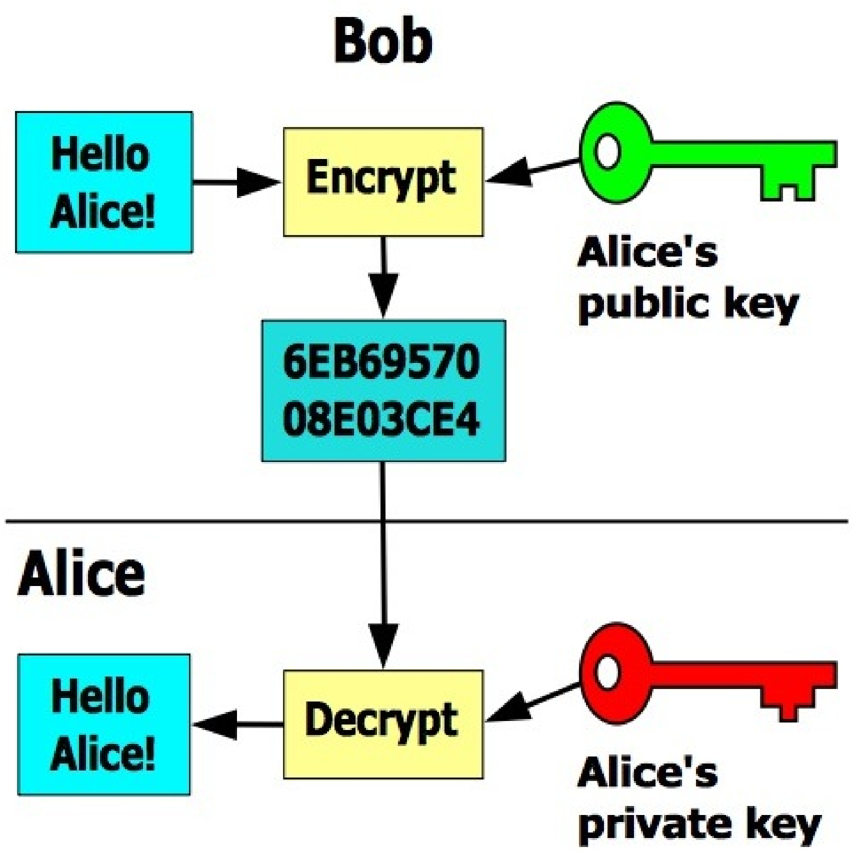
Computer security

Asymmetric encryption

Olivier Markowitch

Public key encryption

A public key cryptosystem uses the public key of the recipient to encrypt the plaintext and the recipient used its private key to decrypt the ciphertext



Time complexity function	Size n					
	10	20	30	40	50	60
n	.00001 second	.00002 second	.00003 second	.00004 second	.00005 second	.00006 second
n^2	.0001 second	.0004 second	.0009 second	.0016 second	.0025 second	.0036 second
n^3	.001 second	.008 second	.027 second	.064 second	.125 second	.216 second
n^5	.1 second	3.2 seconds	24.3 seconds	1.7 minutes	5.2 minutes	13.0 minutes
2^n	.001 second	1.0 second	17.9 minutes	12.7 days	35.7 years	366 centuries
3^n	.059 second	58 minutes	6.5 years	3855 centuries	2×10^8 centuries	1.3×10^{13} centuries

Figure 1.2 Comparison of several polynomial and exponential time complexity functions.

Theorems

1. $\forall n \geq 2 : n = p_1^{e_1} \dots p_r^{e_r}$ where, for $i \in [1, r]$, the p_i are primes and $e_i \geq 0$ are integers

2. If $a, b \in \mathbb{Z}$ are not simultaneously equal to zero, there exist $u, v \in \mathbb{Z}$ such that $au + bv = (a, b)$ where (a, b) denotes the gcd between a and b (Bézout)

3. $ax \equiv 1 \pmod{m} \Leftrightarrow (a, m) = 1$

4. If m is prime and $(a, m) = 1$: $a^{m-1} \equiv 1 \pmod{m}$ (Fermat)

5. Euler Phi function: we note $\Phi(n)$ the number of integers smaller than n and that are prime with n. $\Phi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

6. multiplicative group: $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n$ such that $(a, n) = 1\}$

7. We consider a group composed by $\phi(n)$ elements $(n > 2)$, for an element a of this group we have $a^{\Phi(n)} = 1$

8. We consider a group composed by $\phi(n)$ elements $(n > 2)$, for an element a of this group we have that the order of a divides the order of the group

Example 1

$n = 7, \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}, \phi(7) = 6$

order of 1 = 1 : $1^0 = 1$, $1^1 = 1$

order of 2 = 3 : $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 1$

order of 3 = 6 (generator) : $3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$

order of 4 = 3 : $4^0 = 1$, $4^1 = 4$, $4^2 = 2$, $4^3 = 1$

order of 5 = 6 (generator) : $5^0 = 1$, $5^1 = 5$, $5^2 = 4$, $5^3 = 6$, $5^4 = 2$, $5^5 = 3$, $5^6 = 1$

order of 6 = 2 : $6^0 = 1$, $6^1 = 6$, $6^2 = 1$

Example 2

$n = 9$, $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$, $\phi(9) = 6$

order of 1 = 1 : $1^0 = 1$, $1^1 = 1$

order of 2 = 6 (generator) : $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 7$, $2^5 = 5$, $2^6 = 1$

order of 4 = 3 : $4^0 = 1$, $4^1 = 4$, $4^2 = 7$, $4^3 = 1$

order of 5 = 6 (generator) : $5^0 = 1$, $5^1 = 5$, $5^2 = 7$, $5^3 = 8$, $5^4 = 4$, $5^5 = 2$, $5^6 = 1$

order of 7 = 3 : $7^0 = 1$, $7^1 = 7$, $7^2 = 4$, $7^3 = 1$

order of 8 = 2 : $8^0 = 1$, $8^1 = 8$, $8^2 = 1$

Chinese remainder theorem

Si $\forall 1 \leq i \neq j \leq k : (m_i, m_j) = 1$:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

has one and only one solution modulo $m = m_1 \dots m_k$

Chinese remainder theorem

The solution is unique

since $x \equiv a_i \pmod{m_i}$ and $y \equiv a_i \pmod{m_i}$ $\forall i \in [1, k]$:

$x \equiv y \pmod{m_i}$ $\forall i \in [1, k]$,

m_i divides $x - y$ $\forall i \in [1, k]$,

m divides $x - y$,

$x \equiv y \pmod{m}$

Chinese remainder theorem

The solution exists

Let $M_i = \frac{m}{m_i}\ \forall i \in [1, k]$,

m_i is prime with all m_j (when $i \neq j$),

then m_i is prime with M_i

therefore, it exists an integer c_i such that $c_i M_i \equiv 1 \pmod{m_i}$

Let $x = \sum_{i=1}^{k} a_i c_i M_i$,

We have $x \mod m_i = a_i c_i M_i \mod m_i = a_i$

Indeed, $M_j \equiv 0 \pmod{m_i}$ when $i \neq j$ and $c_i M_i \equiv 1 \pmod{m_i}$

x is a solution of the system

Square roots of 1

$n = pq$ xhere p et q are two primes, it exists four square roots of 1 modulo n

These four square roots are computed from two square roots of 1 modulo p (1 and -1) and two square roots of 1 modulo q (1 and -1) that are combined using the chinese remainder theorem

Square roots of 1

Let $p = 7$, $q = 3$ ($n = 21$), we are looking for a x such that $x^2 = 1 \pmod{n}$. The system of four equations is:

$$(1)\ x \equiv 1 \pmod{p} \text{ et } x \equiv 1 \pmod{q}\,;$$

$$(2)\ x \equiv -1 \pmod{p} \text{ et } x \equiv 1 \pmod{q}\,;$$

$$(3)\ x \equiv 1 \pmod{p} \text{ et } x \equiv -1 \pmod{q}\,;$$

$$(4)\ x \equiv -1 \pmod{p} \text{ et } x \equiv -1 \pmod{q}$$

we solve them using the chinese remainder theorem where $m_1 = p$, $m_2 = q$, $M_1 = \frac{pq}{p} = q$, $M_2 = \frac{pq}{q} = p$, $C_1 = M_1^{-1} \bmod m_1 = 5$ et $C_2 = M_2^{-1} \bmod m_2 = 1$

$$(1)\ x = a_1C_1M_1 + a_2C_2M_2 = 1 \cdot 3 \cdot 5 + 1 \cdot 7 \cdot 1 = 1 \bmod 21$$

$$(2)\ x = a_1C_1M_1 + a_2C_2M_2 = (-1) \cdot 3 \cdot 5 + 1 \cdot 7 \cdot 1 = 8 \bmod 21$$

$$(3)\ x = a_1C_1M_1 + a_2C_2M_2 = 1 \cdot 3 \cdot 5 + (-1) \cdot 7 \cdot 1 = -8 \bmod 21$$

$$(4)\ x = a_1C_1M_1 + a_2C_2M_2 = (-1) \cdot 3 \cdot 5 + (-1) \cdot 7 \cdot 1 = -1 \bmod 21$$

Quadratic residues

$a \in \mathbb{Z}_n^*$ is a quadratic residue modulo n, if it exists $x \in \mathbb{Z}_n^*$ such that $x^2 \equiv a \pmod{n}$. If such a x doesn't exists a is said to be a non quadratic residue modulo n

The set of all the quadratic residues modulo n est noted Q_n. The set of all the non quadratic residues modulo n is noted $\bar{Q_n}$

$\frac{p-1}{2}$ elements of $\mathbb{Z}_p^*$ are squares modulo p and $\frac{p-1}{2}$ elements of $\mathbb{Z}_p^*$ are not squares (where p is a odd prime)

Legendre symbol

Adrien-Marie Legendre

If p is an odd prime and a is an integer, then the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } a \\ 1 & \text{si } a \in Q_p \\ -1 & \text{si } a \in \bar{Q}_p \end{cases}$$

Moreover: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$

Legendre symbol

Proof :

If p divides a, it exists k such that $a = kp$ and $a \equiv 0 \pmod{p}$; therefore $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$

if $a \in Q_p$, it exists $x \in \mathbb{Z}_p$ such that $x^2 \equiv a \pmod{p}$, therefore

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p} \text{ (Fermat)}$$

Legendre symbol

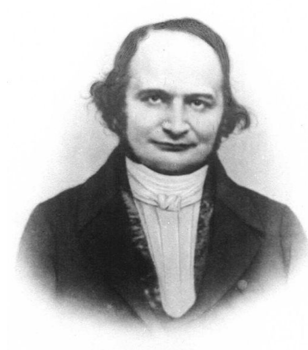
If $a \in \bar{Q}_p$, we have (when p is prime) $a^{p-1} \equiv 1 \pmod{p}$ (Fermat). Then $a^{p-1} - 1 \equiv 0 \pmod{p}$ and

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

Since $a \in \bar{Q}_p$ we haven't $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ (otherwise a would be in Q_p)

Therefore we have $a^{\frac{p-1}{2}} + 1 = 0 \pmod{p}$, and $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ if $a \in \bar{Q}_p$

Jacobi Symbol



Charles Gustave Jacob Jacobi

Let a be an interger and n an odd integer $\geq$ 3 such that $n = p_1^{e_1} \dots p_r^{e_r}$:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}$$

Theorem

1. $a \in Q_n \Leftrightarrow a \in Q_p$ et $a \in Q_q$ (where $n = pq$ and p, q are distinct primes)

2. If $a \in Q_p$ and $a \in \bar{Q}_q$, then $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1 \cdot -1 = -1$

3. Idem, if $a \in \bar{Q}_p$ and $\in Q_q$

4. if $a \in Q_p$ and $a \in Q_q$ then $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1 \cdot 1 = 1$

5. But if $a \in \bar{Q_p}$ and $a \in \bar{Q_q}$ then we have $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = -1 \cdot -1 = 1$

6. Therefore $\left(\frac{a}{n}\right) = 1$ does not allow to know whether $a \in Q_n$ or $a \in \bar{Q_n}$

Factorization

Having a positive integer n, we have to find its prime factors:

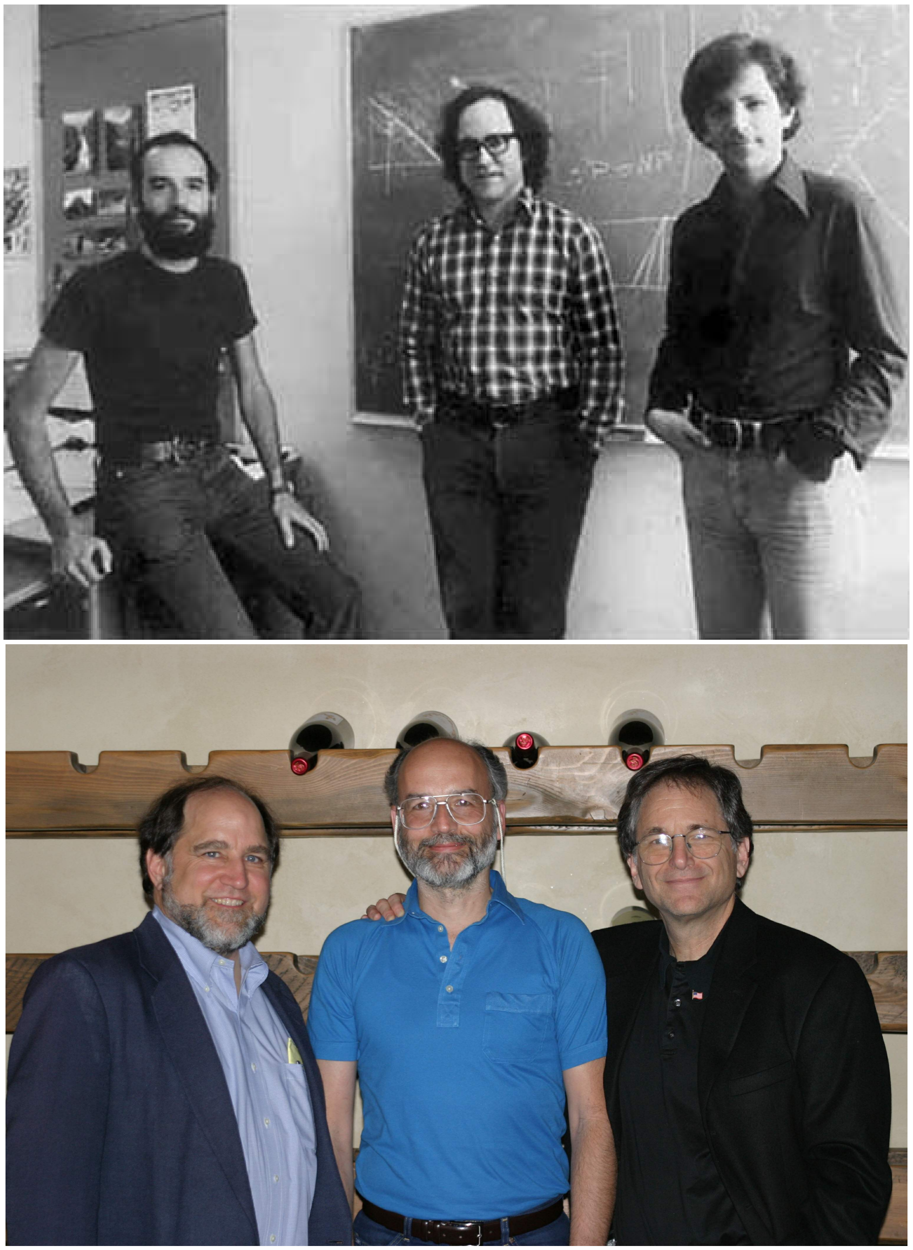
$$n = p_1^{e_1} \dots p_n^{e^n}$$

where p_i are distinct and $e_i \geq 1$

Existing methods:

- ρ-Pollard
- $p - 1$-Pollard
- Crible quadratique
- Number field sieve

RSA



Ronald Rivest - Adi Shamir - Leonard Adleman

RSA

Keys generation

1. choose randomly two large distinct primes p and q approximately of the same size
2. compute $n = pq$ and $\phi(n) = (p-1)(q-1)$
3. choose randomly an integer $e \in \,]1, \phi(n)[$ such that $(e, \phi(n)) = 1$
4. compute the unique $d \in \,]1, \phi(n)[$ such that $e \cdot d \equiv 1 \pmod{\phi(n)}$

The public key is (n, e)
The private key is d

RSA

Encryption
Let $x \in \mathbb{Z}_n$ the message to encrypt. We compute:

$$y = x^e \mod n$$

Decryption
y is decrypted by computing:

$$x = y^d \mod n$$

RSA: keys usage

Knowing the public key (e, n) and the corresponding private key d, n can be factorized

Proof: we have $ed \equiv 1 \pmod{\phi(n)}$

For every integer $a \in \mathbb{Z}_n^*$ we have $a^{ed-1} \equiv 1 \pmod{n}$

We can write: $ed - 1 = 2^s t$ with t an odd integer ($a^{2^s t} \equiv 1 \pmod{n}$)

If $z = a^{2^{s-1} t}$ is a trivial square root of 1 modulo n we choose another integer a

Otherwise (z being a non-trivial square roor of 1 modulo n) we have $z^2 \equiv 1 \pmod{n}$ and n divides $z^2 - 1$, therefore n divides $(z-1)(z+1)$

RSA: keys usage

What are the values of $(z-1,n)$ and $(z+1,n)$?

These two gcd's can have only the following values: 1, p, q or n

Neither can be equal to n, because if $(z-1,n)=n$ then $z-1$ is a multiple of n, and $z \equiv 1 \pmod{n}$ and z is a trivial sqaure root of 1. The same reasoning is valid if $(z+1,n)=n$

These two gcd's cannot be simultaneously equal to 1, because if $(z-1,n)=1$ and $(z+1,n)=1$ then n does not divide z^2-1

Conclusion: at least one of these two gcd's is equal to p ou q

Corollary: two RSA users cannot have the same n in their public key

RSA: cyclic attack

Alice sends to Bob a ciphertext y encrypted with his RSA public key (e_B, n_B)

Oscar observes y (on the communication channel) and knows that Bob is the recipient; Oscar can encrypt again the ciphertext with the public key of Bob until he obtains a cycle:

y^{e_B} mod n_B
$(y^{e_B})^{e_B}$ mod $n_B = y^{e_B^2}$ mod n_B
$\ldots$
$(y^{e_B^{i-2}})^{e_B}$ mod $n_B = y^{e_B^{i-1}}$ mod n_B
$(y^{e_B^{i-1}})^{e_B}$ mod $n_B = y^{e_B^{i}}$ mod n_B

until $y^{e_B^{i}}$ mod $n_B = y$

then Oscar retrieves $x = y^{e_B^{i-1}}$ mod n_B

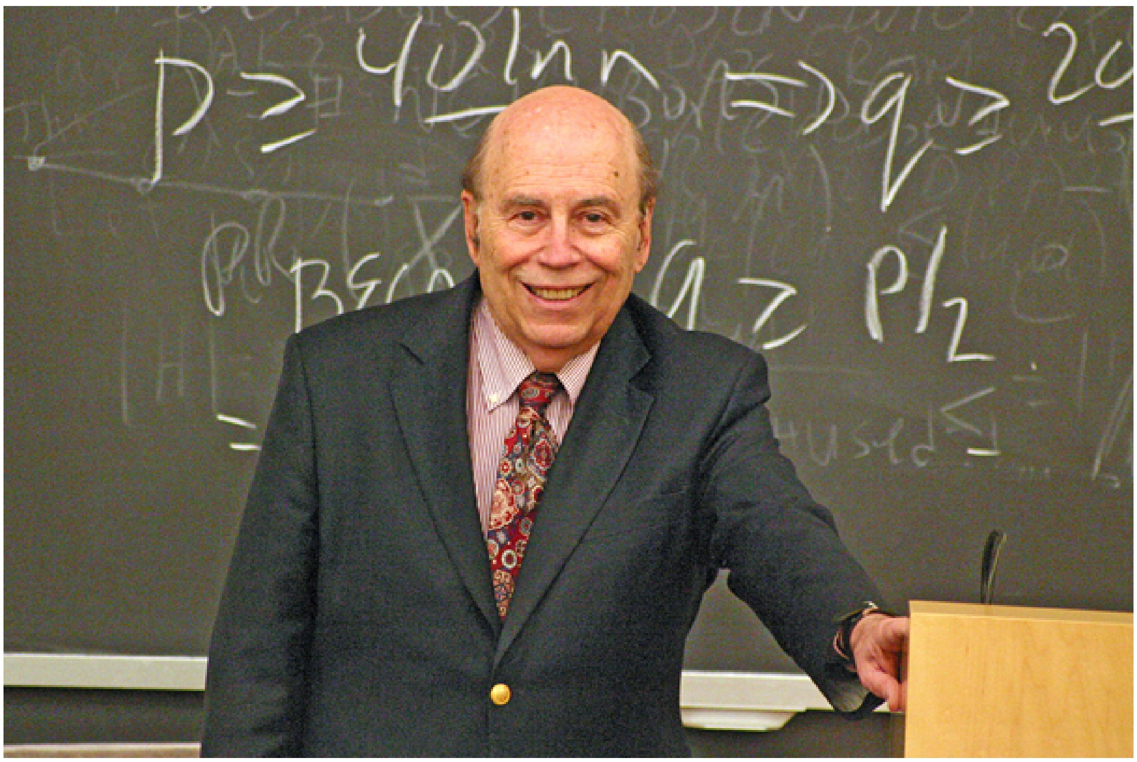
Square root problem

On the basis of n where $n = pq$ and p, q are primes, and having a a quadratic residue modulo n, find a square root of a modulo n

If p and q are known, it exists a solution that has a polynomial complexity

The square root probleme is computationally equivalent to the factorization problem

Rabin



Michael Rabin

Rabin

Keys generation
choose randomly two large distinct primes p and q approximately of the same size and compute $n = pq$

The public key is n
The private key is (p, q)

Encryption
Let $x \in \mathbb{Z}_n$ the message to encrypt. We compute:

$$y = x^2 \mod n$$

Decryption
Compute the four square roots modulo n of y and choose (possibly on the basis of a redundancy) the square root that corresponds to the plaintext

Computation of the four square roots

Suppose $n = pq$ and $p \equiv q \equiv 3 \pmod 4$

- find the integers a and b such that $ap + bq = 1$ (Bezout)
- computer $r = y^{\frac{p+1}{4}} \bmod p$
- computer $s = y^{\frac{q+1}{4}} \bmod q$
- computer $g = aps + bqr \bmod n$
- computer $h = aps + bq(-r) \bmod n$

The four square roots of y modulo n are g, $-g$, h et $-h$

Rabin: chosen cipher text attack

Suppose that Oscar can access a decryption device that decrypt all messages encrypted for Bob

Oscar chooses randomly $x \in Z_n$ and encrypts x for Bob: $y = x^2 \bmod n$. Then, he submits y to the decryption device and obtains, as output, x' (one of the four square roots of y)

With a probability $\frac{1}{2}$, this square root is different from x and $-x$ (otherwise Oscar restarts the process)

We have:

$$x \text{ de la forme } aps + bqr$$

$$x' \text{ de la forme } aps + bq(-r)$$

Oscar computes:

$$\left(x - x', n\right) = (2bqr, pq) = q$$

Rabin: example

Let $p = 277$, $q = 331$
$n = p \cdot q = 91687$

Bob's public key: $n = 91687$
Bob's private key: $(p, q) = (227, 331)$

Alice wants to send the message x to Bob:

$$x_0 = 1001111001$$

She adds a redundancy (duplication of the six last bits):

$$x = x_0 111001 = 1001111001\mathbf{111001} = 40569$$

She computes:

$$y = x^2 \bmod n = 40569^2 \bmod 91687 = 62111$$

Rabin: example

To decrypt the ciphertext y, Bob computes the square roots of y modulo n (Bob knows p and q):

$\sqrt{y}$ mod $n =$

$$\begin{cases} x_1 = 69654 = 10001000000010110 \\ x_2 = 22033 = 101011000010001 \\ x_3 = 40569 = 1001111001111001 \\ x_4 = 51118 = 1100011110101110 \end{cases}$$

Only x_3 has the correct redundancy therefore $x_0 = 1001111001$

Discrete logarithm problem

Suppose a prime p, a generator $\alpha \in \mathbb{Z}_p^*$ and $\beta \in \mathbb{Z}_p^*$; find x, $0 \leq x \leq n-1$ such that $\alpha^x = \beta$

Existing methods:

- baby step, giant step
- ρ-Pollard for logarithms
- Pohlig-Hellman
- Index calculus

El Gamal

Taher El Gamal

El Gamal

Keys generation

1. choose randomly a larte prime p

2. find a generator α of the multiplicative group $\mathbb{Z}^*{}_p$

3. choose randomly an integer $a \in [1, p-2]$

4. compute $\beta = \alpha^a \mod p$

The public key is (p, α, β)
The private key is a

El Gamal

Encryption

To encrypt $x \in \mathbb{Z}_p$, choose randomly an integer $k \in [1, p-2]$ and compute:

$$\begin{cases} y_1 = \alpha^k \mod p \\ y_2 = x \cdot \beta^k \mod p \end{cases}$$

Decryption

Let (y_1, y_2) be the ciphertext:

$$x = {y_1}^{-a} \cdot y_2 \mod p$$

Quadratic residuosity problem

Suppose an odd non prime integer n and $a \in \mathbb{Z}_n^*$ such that $\left(\frac{a}{n}\right) = 1$, is a a quadratic residue modulo n?

The quadratic residuosity problem $\leq_P$ the factorization problem

Goldwasser-Micali

Shafi Goldwasser - Silvio Micali

Goldwasser-Micali

Keys generation

1. choose randomly two large distinct primes p and q approximately of the same size
2. compute $n = pq$
3. choose $z \in \mathbb{Z}_n$ such that z is a non-quadratic residue modulo n and such that $\left(\frac{z}{n}\right) = 1$

The public key is (n, z)
The private key is (p, q)

Goldwasser-Micali

Encryption
Let x be composed by t bits: $x_1 \ldots x_t$

1. choose randomly $\forall i \in [1, t]$: r_i

2. $\forall i \in [1, t] : y_i = z^{x_i} \cdot {r_i}^2 \mod n$

Decryption
$\forall i \in [1, t]$, compute $\left(\frac{y_i}{p}\right) = e_i$

If $e_i = 1$ then $x_i = 0$, otherwise $x_i = 1$

Remark : y_i is a quadratic residue modulo n ($n = pq$) if y_i is a quadratic residue modulo p

Goldwasser-Micali

Let $p = 7$, $q = 3$ and therefore $n = 21$) be the private and public information of Bob

We look for a $z \in \mathbb{Z}_n$ that is a non-quadratic residue modulo n and such that $\left(\frac{z}{n}\right) = 1$

The quadratic residue modulo 21 are:
$\{1, 4, 7, 9, 15, 16, 17, 18\}$

Let's try $z = 11$ and compute $\left(\frac{11}{21}\right)$ = $\left(\frac{11}{3}\right) \cdot \left(\frac{11}{7}\right)$ = $(11^1 \mod 3) \cdot (11^3 \mod 7) = -1 \cdot 1 = -1$. Therefore $z = 11$ is not appropriate

Let's try $z = 5$: $\left(\frac{5}{21}\right) = \left(\frac{5}{3}\right) \cdot \left(\frac{5}{7}\right) = (5^1 \mod 3) \cdot (5^3 \mod 7) = -1 \cdot -1 = 1$. Therefore $z = 5$ is ok

Goldwasser-Micali

Alice wants to encrypt $x = 10110$ for Bob

she chooses randomly $r_1 = 4$, $r_2 = 8$, $r_3 = 13$, $r_4 = 5$ and $r_5 = 4$

She computes:
$y_1 = 5 \cdot 4^2 = 80 = 17 \mod 21$
$y_2 = 8^2 = 1 \mod 21$
$y_3 = 5 \cdot 13^2 = 845 = 5 \mod 21$
$y_4 = 5 \cdot 5^2 = 125 = 20 \mod 21$
$y_5 = 4^2 = 16 \mod 21$

The cipher text is $y = (17, 1, 5, 20, 16)$.

Goldwasser-Micali

To decrypt $y = (17, 1, 5, 20, 16)$ Bob computes the following Legendre symbols:

$\left(\frac{y_1}{p}\right) = \left(\frac{17}{7}\right) = 17^3 = 4913 = -1 \mod 7 \neq 1 \to x_1 = 1$
$\left(\frac{y_2}{p}\right) = \left(\frac{1}{7}\right) = 1^3 = 1 \mod 7 \to x_2 = 0$
$\left(\frac{y_3}{p}\right) = \left(\frac{5}{7}\right) = 5^3 = 125 = -1 \mod 7 \neq 1 \to x_3 = 1$
$\left(\frac{y_4}{p}\right) = \left(\frac{20}{7}\right) = 20^3 = 8000 = -1 \mod 7 \neq 1 \to x_4 = 1$
$\left(\frac{y_5}{p}\right) = \left(\frac{16}{7}\right) = 16^3 = 4096 = 1 \mod 7 \to x_5 = 0$

Bob retrieves $x = 10110$

Algorithm Extended Euclidean algorithm

INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: $d = \gcd(a, b)$ and integers x, y satisfying $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a,\ x \leftarrow 1,\ y \leftarrow 0$, and return($d$,$x$,$y$).
2. Set $x_2 \leftarrow 1,\ x_1 \leftarrow 0,\ y_2 \leftarrow 0,\ y_1 \leftarrow 1$.
3. While $b > 0$ do the following:
   - 3.1 $q \leftarrow \lfloor a/b \rfloor,\ r \leftarrow a - qb,\ x \leftarrow x_2 - qx_1,\ y \leftarrow y_2 - qy_1$.
   - 3.2 $a \leftarrow b,\ b \leftarrow r,\ x_2 \leftarrow x_1,\ x_1 \leftarrow x,\ y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a,\ x \leftarrow x_2,\ y \leftarrow y_2$, and return($d$,$x$,$y$).

Algorithm Computing multiplicative inverses in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$.
OUTPUT: $a^{-1} \bmod n$, provided that it exists.

1. Use the extended Euclidean algorithm (Algorithm 2.107) to find integers x and y such that $ax + ny = d$, where $d = \gcd(a, n)$.
2. If $d > 1$, then $a^{-1} \bmod n$ does not exist. Otherwise, return(x).

Algorithm Repeated square-and-multiply algorithm for exponentiation in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$, and integer $0 \leq k < n$ whose binary representation is $k = \sum_{i=0}^{t} k_i 2^i$.
OUTPUT: $a^k \bmod n$.

1. Set $b \leftarrow 1$. If $k = 0$ then return(b).
2. Set $A \leftarrow a$.
3. If $k_0 = 1$ then set $b \leftarrow a$.
4. For i from 1 to t do the following:
   - 4.1 Set $A \leftarrow A^2 \bmod n$.
   - 4.2 If $k_i = 1$ then set $b \leftarrow A \cdot b \bmod n$.
5. Return(b).

Algorithm Finding square roots modulo a prime p

INPUT: an odd prime p and an integer a, $1 \le a \le p-1$.
OUTPUT: the two square roots of a modulo p, provided a is a quadratic residue modulo p.

1. Compute the Legendre symbol $\left(\frac{a}{p}\right)$ using Algorithm 2.149. If $\left(\frac{a}{p}\right) = -1$ then return(a does not have a square root modulo p) and terminate.
2. Select integers b, $1 \le b \le p-1$, at random until one is found with $\left(\frac{b}{p}\right) = -1$. ($b$ is a quadratic non-residue modulo p.)
3. By repeated division by 2, write $p - 1 = 2^s t$, where t is odd.
4. Compute $a^{-1} \bmod p$ by the extended Euclidean algorithm (Algorithm 2.142).
5. Set $c \leftarrow b^t \bmod p$ and $r \leftarrow a^{(t+1)/2} \bmod p$ (Algorithm 2.143).
6. For i from 1 to $s-1$ do the following:
   - 6.1 Compute $d = (r^2 \cdot a^{-1})^{2^{s-i-1}} \bmod p$.
   - 6.2 If $d \equiv -1 \pmod p$ then set $r \leftarrow r \cdot c \bmod p$.
   - 6.3 Set $c \leftarrow c^2 \bmod p$.
7. Return(r, $-r$).

Algorithm Finding square roots modulo n given its prime factors p and q

INPUT: an integer n, its prime factors p and q, and $a \in Q_n$.
OUTPUT: the four square roots of a modulo n.

1. Use Algorithm 3.39 (or Algorithm 3.36 or 3.37, if applicable) to find the two square roots r and $-r$ of a modulo p.
2. Use Algorithm 3.39 (or Algorithm 3.36 or 3.37, if applicable) to find the two square roots s and $-s$ of a modulo q.
3. Use the extended Euclidean algorithm (Algorithm 2.107) to find integers c and d such that $cp + dq = 1$.
4. Set $x \leftarrow (rdq + scp) \bmod n$ and $y \leftarrow (rdq - scp) \bmod n$.
5. Return($\pm x \bmod n$, $\pm y \bmod n$).