ASYMMETRIC CRYPTOGRAPHY

A ← B (LESSON 3)

RECIPIENT SENDER

Main properties

- The encryption function of A, E_A is known to everybody and easy to calculate
- Its inverse function D_A is hard to be computed unless one knows a secret key (that only A knows)

EASY AND HARD

We say that a problem depending on an integer n is "easy" if there is an algorithm that solves it in polynomial time wrt $\log(n)$

$$T(n) \leq C(\log n)^k$$

C, k independent on n

$\log n$ ↑ proportional to the number of digits of n

"hard" = not easy

EXAMPLES OF EASY PROBLEMS

- Given $n = a^b$, find a, b
- Given n, m find $\gcd(n, m)$ (Euclide)
- Given n and a prime to n find $a^{-1} \bmod n$
- Given n, determine if n is prime (AKS primality test)
  → Agrawal Kayal Saxena 2002
- Given a, m, n find $a^m \bmod n$ (discrete power)

Examples of HARD PROBLEMS

- **Discrete logarithm**
  Given N and a prime to N,
  $a^e \bmod N$ $\rightsquigarrow$ find e
- **Discrete root**
  Given N, e, $a^e \bmod N$, find a
- **Factorisation**
  Factorise N
- **Diffie-Hellman problem**
  Given N and a prime to N, a^x, a^y find a^{xy} (breakable if the discrete log does)

ONE WAY FUNCTIONS

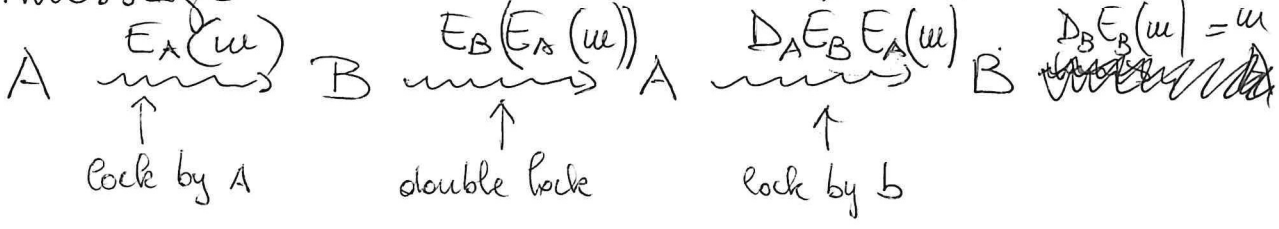
We need functions $E_A : \mathbb{N} \longrightarrow \mathbb{N}$ such that
- the computation of $E_A(n)$ is easy
- the " " $D_A(n)$ is hard

Example: DOUBLE LOCK message exchange
A, B want to send to B an information (secret key)

A $\rightsquigarrow$ E_A, D_A
B $\rightsquigarrow$ E_B, D_B

Assume E_A, E_B commute

message



REMIND ON EULER FUNCTION

$$\varphi(n) = |\mathbb{Z}_n^*|$$

Therefore we have **EULER THEOREM**

$$a^{\varphi(n)} \equiv 1 \mod n, \quad \forall a \text{ s.t. } (a,n)=1$$

- $\varphi(n)$ is multiplicative

$$\begin{cases} \varphi(n \cdot m) = \varphi(n)\varphi(m) & \text{if } (n,m)=1 \\ \varphi(p) = p-1 \\ \varphi(p^e) = p^{e-1}(p-1) \end{cases}$$

- If one knows (the factorization of) $n = p_1^{e_1} \cdots p_k^{e_k}$

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i-1)$$

RSA RIVEST SHAMIR ADLEMAN 1977

1) A chooses two primes p, q distinct and big $n = pq$

2) A computes $\varphi(n) = (p-1)(q-1)$
$= n - p - q + 1$

3) A choose e such that $(e, \varphi(n)) = 1$

4) A computes $d \equiv e^{-1} \bmod \varphi(n)$

Public key of A $\rightsquigarrow (n, e)$
Secret key of A $\rightsquigarrow d$

ENCRYPTION : If B wants to send m to A

$m \in \mathbb{Z}_n^*$ $\quad m < n$

$E_A(m) = m^e \bmod n$

A receives m^e. A knows d, therefore computes

$(m^e)^d = m^{ed} \leftarrow ed = 1 + k\varphi(n)$

$= m^{1+k\varphi(n)} = m\left(m^{\varphi(n)}\right)^k \equiv m \bmod n$

$\|\|$
1 (Euler)

The security of RSA depends on the problem of factorization.

Factorization is easy when

- Prime factor are small
- " " " close each other
- Numbers n s.t. $n-1$ or $n+1$ factorize in small primes.

Therefore the choice of p, q is important.

Fixpoint problems

One must avoid that $m^e = m \mod n$

$$m^{e-1} \equiv 1 \mod n \iff \begin{matrix} \mathrm{ord}_p(m) \mid e-1 \\ \mathrm{ord}_q(m) \mid e-1 \end{matrix}$$

$$\left| \{ m \mid \mathrm{ord}_p(m) \mid e-1 \} \right| = \sum_{k \mid e-1} \left| \{ m \mid \mathrm{ord}_p(m) = k \} \right|$$

$$= \sum_{k \mid (e-1, p-1)} \varphi(k) = (e-1, p-1)$$

The cardinality of the set of fixed points is

$$(e-1, p-1)(e-1, q-1)$$

We need to choose e such that this quantity is small

Cycling attack

We also need to avoid that the encryption function $m \mapsto m^e$ has a period too small, i.e. we need that the smallest k such that $m^{e^k} = m \quad \forall m \in \mathbb{Z}_n^\times$ is "large"

Theorem

Let (n, e) be a public key for RSA.
Let $m \in \mathbb{Z}_n^\times$
Let r be the greatest prime divisor of $p-1$
" l " " " " " $r-1$

Then

$$\mathbb{P}(k \geq l) \geq \left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{e}\right).$$

Therefore we need to choose p, q s.t. $p-1$, $q-1$ have at least a big prime factor r_p, r_q such that $r_p - 1$, $r_q - 1$ have a large prime factor l_p, l_q. ∎