Mathematics and Cryptography

Course no. 4

Jean-Sébastien Coron and David Galindo

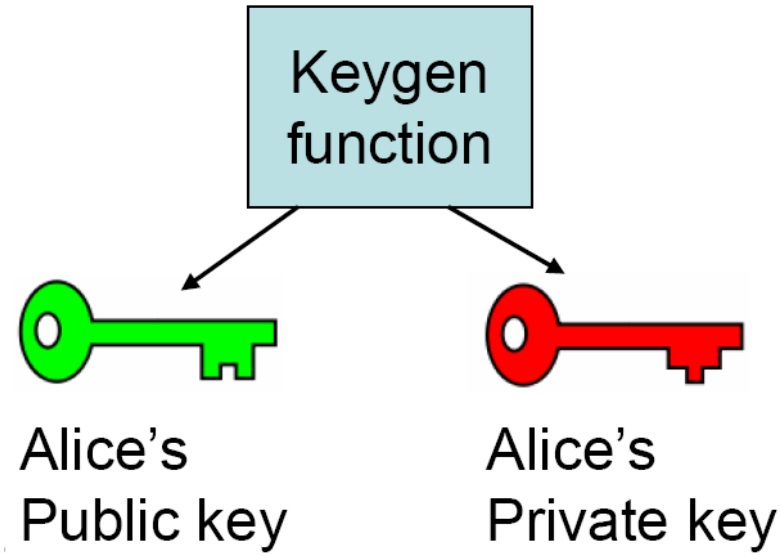
{jean-sebastien.coron,david.galindo}@uni.lu.

Université du Luxembourg

Public-key cryptography

- Invented by Diffie and Hellman in 1976. Revolutionized the field.

- Each user now has two keys
  - A public key PK
  - A public key SK
  - Should be hard to compute the private key from the public key.



Public-key cryptography (II)

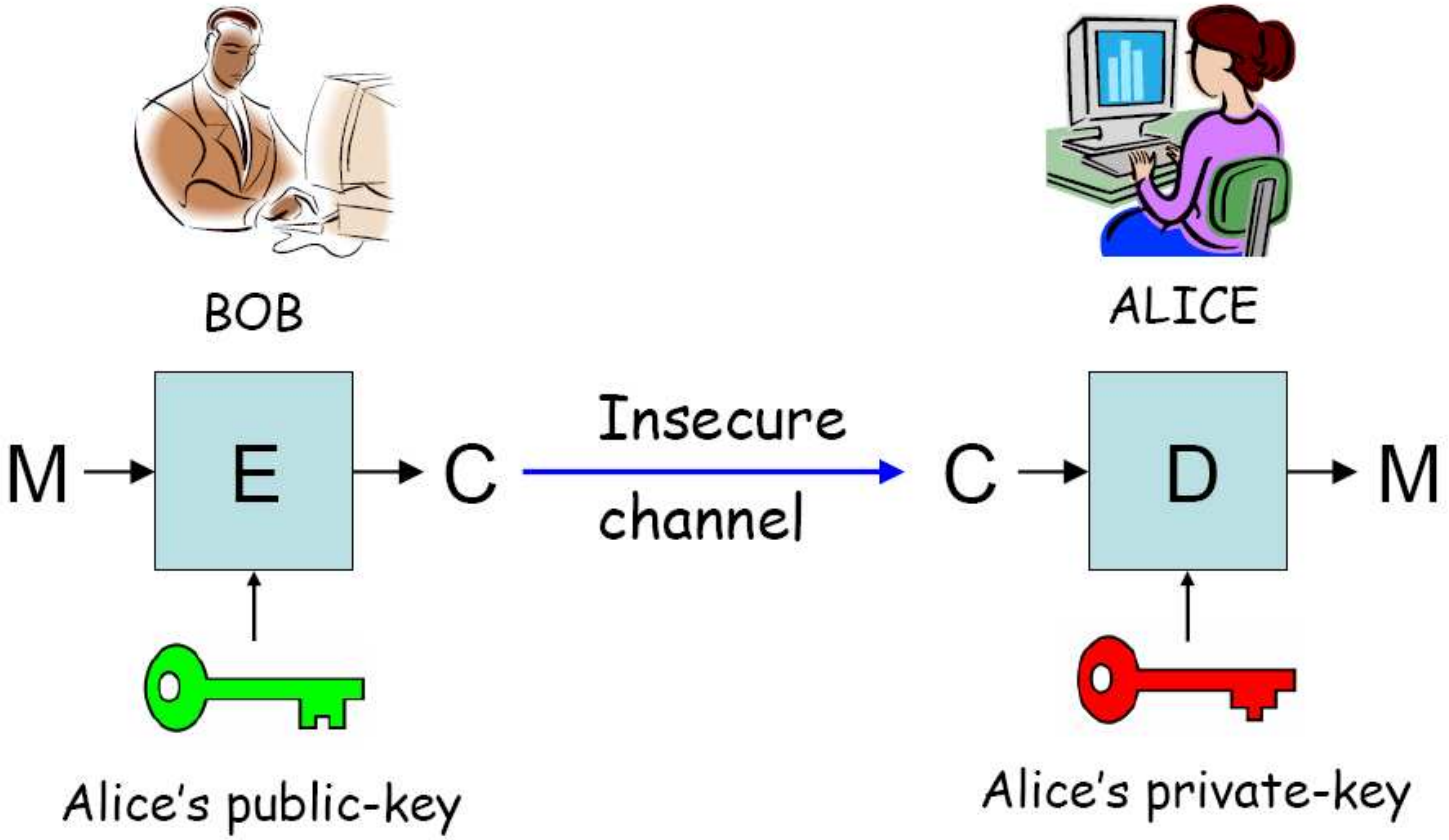
- Should be hard to compute the private key from the public key.

- It enables
  - Asymmetric encryption
  - Digital signatures
  - Key exchange
  - Identification...

  And many other functionalities

Public-key encryption

- Solves the key distribution issue



The RSA algorithm

- The RSA algorithm is the most widely-used public-key encryption algorithm
  - Invented in 1977 by Rivest, Shamir and Adleman.
  - Used for encryption and signature.
  - Widely used in electronic commerce protocols (SSL).
- Public-key encryption: two keys.
  - One key is made public and used to encrypt.
  - The other key is kept private and enables to decrypt.

RSA

- Key generation:
  - Generate two large distinct primes p and q of same bit-size.
  - Compute $n = p \cdot q$ and $\phi = (p-1)(q-1)$.
  - Select a random integer e, $1 < e < \phi$ such that $\gcd(e, \phi) = 1$
  - Compute the unique integer d such that

$$e \cdot d \equiv 1 \mod \phi$$

    using the extended Euclidean algorithm.
  - The public key is (n, e). The private key is d.

RSA encryption

- Encryption
  - Given a message $m \in [0, n-1]$ and the recipent's public-key (n, e), compute the ciphertext:

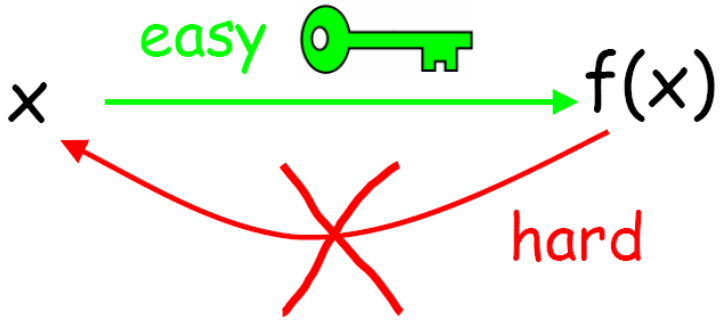
$$c = m^e \mod n$$

- Decryption
  - Given a ciphertext c, to recover m, compute:

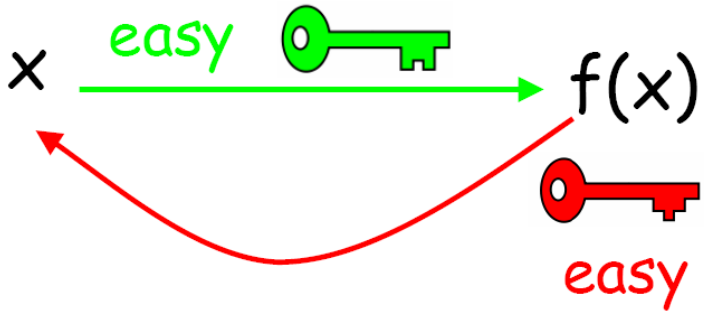
$$m = c^d \mod n$$

RSA: trapdoor one-way permutation

- Trapdoor unknown:



- Trapdoor known:



- Asymmetric encryption:
  - Everybody can encrypt to Alice using PK
  - Only Alice can decrypt using SK

Fermat's little theorem

- Theorem
  - For any prime p and any integer $a \neq 0 \mod p$, we have $a^{p-1} \equiv 1 \mod p$. Moreover, for any integer a, we have $a^p \equiv a \mod p$.

Proof that decryption works

- Since $e \cdot d \equiv 1 \mod \phi$, there is an integer k such that $e \cdot d = 1 + k \cdot \phi$.
- If $m \neq 0 \mod p$, then by Fermat's little theorem $m^{p-1} \equiv 1 \mod p$, which gives :

$$m^{1+k\cdot(p-1)\cdot(q-1)} \equiv m \mod p$$

  - This equality is also true if $m \equiv 0 \mod p$.
  - This gives $m^{ed} \equiv m \mod p$ for all m.
  - Similarly, $m^{ed} \equiv m \mod q$ for all m.
  - By the Chinese Remainder Theorem, if $p \neq q$, then

$$m^{ed} \equiv m \mod n$$

Security of RSA

- The security of RSA is based on the hardness of factoring.
  - Given $n = p \cdot q$, it should be difficult to recover p and q.
  - No efficient algorithm is known to do that. Best algorithms have sub-exponential complexity.
  - Factoring record: a 640-bit RSA modulus n.
  - In practice, one uses 1024-bit RSA moduli.

Attacks against RSA encryption

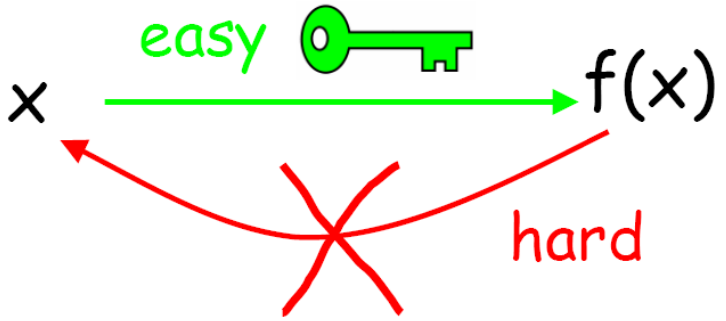
- There are many attacks on basic RSA encryption
  - Coppersmith's attack for small e.
  - Håstad's attack for related messages.
  - If only two possible messages m_0 and m_1, from $c = m_b^e \mod N$ one can easily recover m_b.
- To prevent these attacks:
  - The message m is first padded with fixed blocks and random blocks, then encrypted.
  - Example: PKCS#1 v1.5
    - ✓ $\mu(m) = 0002 \| r \| 00 \| m$
    - ✓ $c = \mu(m)^e \mod N$
  - Better: OAEP (Bellare and Rogaway, 1994)

The RSA signature scheme

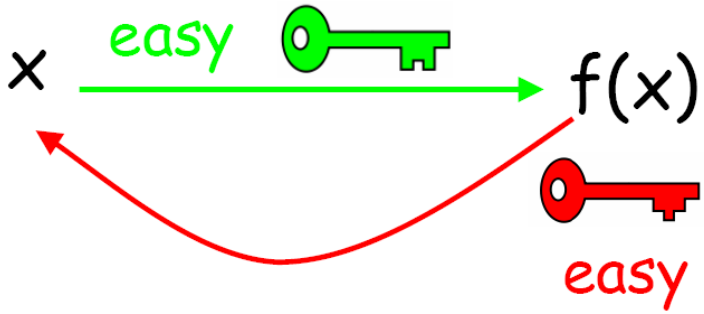
- Key generation :
  - Public modulus: $N = p \cdot q$ where p and q are large primes.
  - Public exponent : e
  - Private exponent: d, such that $d \cdot e = 1 \mod \phi(N)$
- To sign a message m, the signer computes :
  - $s = m^d \mod N$
  - Only the signer can sign the message.
- To verify the signature, one checks that:
  - $m = s^e \mod N$
  - Anybody can verify the signature

RSA: trapdoor one-way permutation

- Trapdoor unknown:



- Trapdoor known:



- Digital signatures:
  - Everybody can verify Alice's signatures using PK
  - Only Alice can sign using SK

Hash-and-sign paradigm

- There are many attacks on basic RSA signatures:
  - Existential forgery: $r^e = m \mod N$
  - Chosen-message attack: $(m_1 \cdot m_2)^d = m_1^d \cdot m_2^d \mod N$
- To prevent from these attacks, one usually uses a hash function. The message is first hashed, then padded.
  - $m \longrightarrow H(m) \longrightarrow \texttt{1001}\ldots\texttt{0101}||H(m)$
  - Example: PKCS#1 v1.5:
    $\mu(m) = \texttt{0001 FF}\ldots\texttt{FF00}||c_{\mathsf{SHA}}||\mathsf{SHA}(m)$
  - ISO 9796-2: $\mu(m) = \mathsf{6A}||m[1]||H(m)||\mathsf{BC}$
  - Better: FDH, PSS (Bellare and Rogaway, 1996)