Théorie algorithmique des nombres

Cours no. 9

Jean-Sébastien Coron

Université du Luxembourg

November 22, 2009

Summary

- Algorithmic number theory.
  - Application of Euler function and Fermat's little theorem: the RSA algorithm

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.

Public-key encryption

- Alice wants to send a message to Bob:
  - She encrypts it using Bob's public-key.
  - Only Bob can decrypt it using his own private-key.
  - Alice and Bob do not need to meet to establish a secure communication.
- Security:
  - It must be difficult to recover the private-key from the public-key
  - but not enough in practice.

- 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:

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

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.