Classical Cryptography

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

2. Tutorial: Rivest, Shamir and Adleman

As the title says, this tutorial will focus on the RSA cryptosystem, widely used for *asymmetric cryptography*.

Given an integer n as the security parameter, RSA works in three stages:

Key setup Each user (here, Alice) computes her own public and private keys:

- Choose two distinct primes p and q at random, such that $2^{n/2-1} < p, q < 2^{n/2}$ and $2^{n-1} < p \cdot q < 2^n$.
- Compute $N = p \cdot q$ and $\varphi(N) = (p-1)(q-1)$.
- Choose an integer e in $\{2, \ldots, \varphi(N)-2\}$ at random, coprime to $\varphi(N)$.
- Compute $d = e^{-1} \bmod \varphi(N)$, the multiplicative inverse of e modulo $\varphi(N)$.
- Publish the public key $K = (N, e)$ and securely store the private key $S = (N, d)$.
- Forget p, q and $\varphi(N)$.

Encryption Bob knows Alice's public key (N, e) and wants to send her the plaintext message x, where x is an integer and $x < 2^{n-1}$:

- Compute and send $y = x^e \bmod N$.

Decryption Alice knows her own private key (N, d) and wants to decrypt the ciphertext y:

- Compute $x^* = y^d \bmod N$.

Exercise 2.1 (A simple example).

Let's take the security parameter $n = 6$ bits and choose $p = 5$ and $q = 11$. We also pick $e = 13$.

(i) Finish the key setup: compute Alice's public and private keys.

(ii) Bob wants to send the plaintext $x = 6$ to Alice. Compute the corresponding ciphertext y.

(iii) Decrypt the ciphertext y using Alice's private key.

Exercise 2.2 (Correctness of RSA).

We want to prove here that the decrypted plaintext x^* corresponds to the original message x.

(i) Prove that for any $a \in \mathbb{Z}_p$ and any integer k, we have $a^{k(p-1)+1} = a$.
Hint: Fermat's Little Theorem.

(ii) Show that $ed - 1$ is a multiple of $p - 1$ and of $q - 1$.

(iii) Taking $a \in \mathbb{Z}_p$, prove that $a^{ed} = a$. Same question for $b \in \mathbb{Z}_q$.

(iv) Compute $x^{ed} \bmod p$ and $x^{ed} \bmod q$ in function of $a = x \bmod p$ and $b = x \bmod q$.

(v) Show that $x^{ed} \equiv x \bmod N$.
Hint: Chinese Remainder Theorem.

Exercise 2.3 (Extending RSA).

For now, RSA works with plaintext messages of $n - 1$ bits. Suppose now that we have an M-bit message to encrypt.

(i) How can we do that?

(ii) Is it a good solution?

(iii) Another idea?

Exercise 2.4 (Security parameter).

As of today, the security of RSA relies on the hardness of factoring N, which is an n-bit number.

Currently, the best known algorithm to factor large integers is the Number Field Sieve, which requires approximately $L(n)$ operations to factor an n-bit number, with

$$L(n) = 2^{1.9229 \cdot n^{1/3} \cdot (\log_2 n)^{2/3}}.$$

Cryptographic recommendations state that a problem is currently intractable if it requires at least 2^80 operations.

(i) Compute $L(512)$, $L(1024)$, $L(2048)$.

(ii) What security parameter should you choose?