Public Key Cryptography

Cryptography and Protocols

Andrei Bulatov

Asymmetric Encryption Schemes

- Main idea: Use two keys, public and private
- Everyone can encrypt, but to decrypt one needs the private key
- Useful if we need to communicate with someone we don't have any preliminary agreements
- Usually slower and more expensive than private cryptography
- This defines usual applications:
  - key distribution
  - digital signatures
  - …

Asymmetric Encryption Schemes (cntd)

- **Definition**

An asymmetric encryption scheme (AES) is a triple of algorithms (K, E, D):

- keys: (e, d) e is a public encryption key
  d is a private decryption key
- encryption: $E_{e(P)} = C$
- decryption: $D_d(C) = P$

Trapdoor Functions

- Requirement to a AES: it has to be a trapdoor function:
  - All algorithms are polynomial time (efficient)
  - K: is a randomized algorithm
  - E_e: is a permutation on some set S

    (sometimes it is required that S is efficiently sampleable)
  - $D_d\left(E_e(P)\right) = P$ for all $P \in S$
  - for each e generated by K, E_e is a one-way permutation

even if the adversary knows e

That is for some superpolynomial pair (T, ε), for any Eve of time complexity at most T

$$\Pr_{\substack{(e,d)\leftarrow K \\ P\leftarrow S}}\left[\text{Eve}\left(e, E_e(P)\right) = P\right] < \varepsilon$$

Candidates: RSA

- Invented in 1977 by Rabin, Shamir and Adleman
- K: choose random primes p, q of length k
  $n = p \cdot q$. Note that $\varphi(n) = (p-1)(q-1)$
  choose e at random from $\mathbb{Z}^*_{\varphi(n)}$
- Public key: n, e
- Private key: d such that $d = e^{-1}(\mathrm{mod}\ \varphi(n))$
  that is $e \cdot d = m \cdot \varphi(n) + 1$
- Encryption: $\mathrm{RSA}_{n,e}(P) \equiv P^e(\mathrm{mod}\ n)$
- $\mathrm{RSA}_{n,e}$ is a permutation on $\mathbb{Z}^*_n$. Indeed, let $C \equiv P^e(\mathrm{mod}\ n)$
  $C^d \equiv P^{ed} \equiv P^{m\varphi(n)+1} \equiv P\ (\mathrm{mod}\ n)$
- Decryption: $P \equiv C^d\ (\mathrm{mod}\ n)$
- RSA assumption: RSA is a trapdoor function

The Chinese Remainder Theorem

Theorem

Let $m_1, m_2, \dots, m_k$ be pairwise relatively prime positive integers and $a_1, a_2, \dots, a_k$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdot \dots \cdot m_k$.
(That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Garner's Formula

- Suppose

$$x \equiv a \pmod{p}$$

$$x \equiv b \pmod{q}$$

Then $x = \Big((a-b)\cdot\big(q^{-1} \bmod p\big)\Big)\cdot q + b$

- Check.

Candidates: Rabin Trapdoor Permutation

- It is not a permutation. But it is a permutation on quadratic residues

  A quadratic residue modulo n is a number $t \equiv s^2 (\mathrm{mod}\, n)$
- K: choose p, q, random primes of length m with $p, q \equiv 3 (\mathrm{mod}\, 4)$, $n = p \cdot q$.

  Note that $\varphi(n) = (p-1)(q-1) = (4k+2)(4k'+2) = 4k''$
- Public key: n
- Private key: p, q
- Encryption: $\mathrm{RABIN}_n(P) \equiv P^2 (\mathrm{mod}\, n)$

  RABIN_n is a permutation on the set of quadratic residues.

Candidates: Rabin Trapdoor Permutation (cntd)

- Decryption: $C = \mathrm{RABIN}_n(P) \equiv P^2 (\mathrm{mod}\, n)$

  If $p = 4k + 3$ and $q = 4k' + 3$ then let $P_1 = C^{k+1}$ and $P_2 = C^{k'+1}$

  We show that $P_1 \equiv P (\mathrm{mod}\, p)$ and $P_2 \equiv P (\mathrm{mod}\, q)$

  Note that $P \equiv S^2 (\mathrm{mod}\, n)$

  Therefore

  $P_1 = \left(P^2\right)^{k+1} \equiv S^{4(k+1)} \equiv S^{p-1+2} \equiv S^2 \equiv P (\mathrm{mod}\, p)$

  Then use Chinese Remainder Theorem

- Inverting Rabin's function is equivalent to factoring Blum integers
- A Blum integer is a number $n = p \cdot q$ with $p, q \equiv 3 (\mathrm{mod}\, 4)$