The RSA Cryptosystem

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **The RSA Cipher**
- **Quadratic Residues**

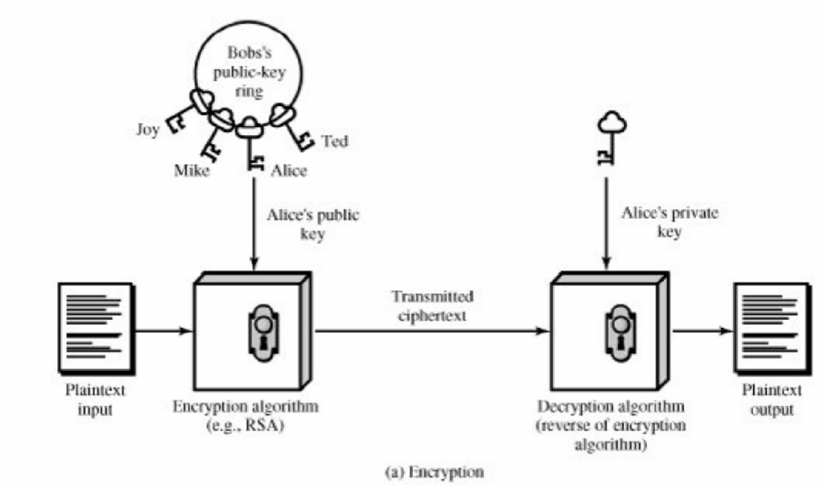
Public Key Cryptography

- **Two keys**
  - **Sender uses recipient's public key to encrypt**
  - **Receiver uses his private key to decrypt**
- **Based on trap door, one way function**
  - **Easy to compute in one direction**
  - **Hard to compute in other direction**
  - **"Trap door" used to create keys**
  - **Example: Given p and q, product N=pq is easy to compute, but given N, it is hard to find p and q**

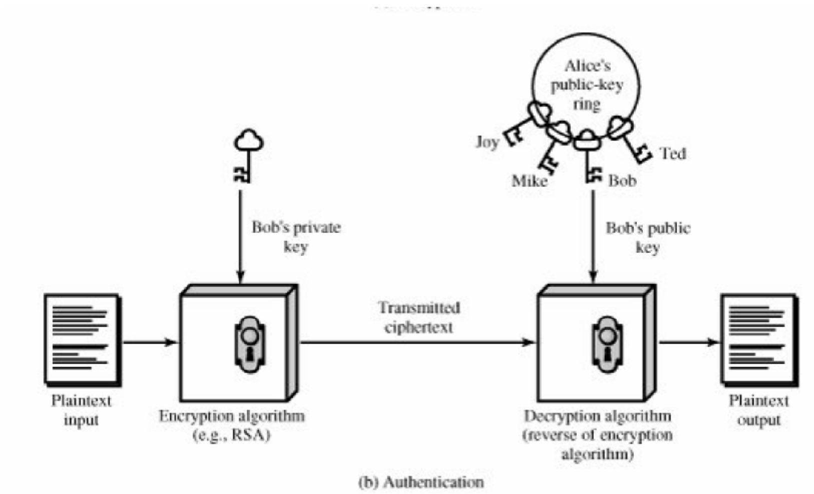
Public Key Cryptography

- Encryption
  - **Suppose we encrypt M with Bob's public key**
  - **Only Bob's private key can decrypt to find M**
- Digital Signature
  - **Sign by "encrypting" with private key**
  - **Anyone can verify signature by "decrypting" with public key**
  - **But only private key holder could have signed**
  - **Like a handwritten signature**

Encryption



Authentication



The RSA

RSA Cryptosystem

Let $n = pq$, where p and q are primes. Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, and define

$$\mathcal{K} = \{(n, p, q, a, b) : ab \equiv 1 \pmod{\phi(n)}\}.$$

For $K = (n, p, q, a, b)$, define

$$e_K(x) = x^b \bmod n$$

and

$$d_K(y) = y^a \bmod n$$

($x, y \in \mathbb{Z}_n$). The values n and b comprise the public key, and the values p, q and a form the private key.

Proof of Correctness

$ab \equiv 1(\bmod\ \phi(\mathrm{n})) \Rightarrow \mathrm{ab}=1+\mathrm{t}\phi(\mathrm{n})$

for some integer $\mathrm{t} \geq 1$.

Suppose, $x \in Z_n^* \Rightarrow x^{ab} \equiv x^{1+t\phi(n)} \equiv x(x^{\phi(n)})^t \equiv x\ (\bmod\ \mathrm{n})$

[follows from Euler's Theorem]

Now, consider $\mathrm{x} \in Z_n \setminus Z_n^*$

$So, \gcd(x,n) \neq 1 \Rightarrow (x$ is a multiple of $p)$or$(x$ is a multiple of $q)$

Thus, gcd(x,p)=p or gcd(x,q)=q

If gcd(x,p)=p, then gcd(x,q)=1

[as otherwise x is a multiple of both p and q and still
x is less than n=pq]

Proof of Correctness

Thus, $x^{\phi(q)} \equiv 1(\text{mod } q) \Rightarrow x^{t\phi(q)} \equiv 1(\text{mod } q)$

$\Rightarrow x^{t\phi(q)\phi(p)} \equiv 1(\text{mod } q)$

$\Rightarrow x^{t\phi(n)} \equiv 1(\text{mod } q)$

Thus, $x^{t\phi(n)} = 1 + kq,$

where k is a positive integer

Multiplying both sides by x,

$x^{t\phi(n)+1} = x + kqx$

$\because \gcd(x, p) = p \Rightarrow x = cp,$ for some positive integer c

$x^{t\phi(n)+1} = x + kcpq$

$\Rightarrow x^{t\phi(n)+1} \equiv x^{ab} \equiv x(\text{mod n})$

Similarly, we can prove when gcd(x,q)=q

Example

- **Bob chooses p=101 and q=113**
  - **Thus n=11413**
  - **Φ(n)=100x112=11200=$2^6 5^2 7$**
  - **b can be used for encryption if and only if it is not a multiple of 2, 5 or 7. Let b=3533**
- **In practice Bob will not factor Φ(n), but will check whether gcd(b, Φ(n))=1 using EA and compute b^{-1} at the same time.**

Examples

- **Bob publishes n=11413 and b=3533.**
- **Suppose Alice wants to encrypt x=9726 and send to Bob.**
- **Hence, she computes x^b(mod n) $=9726^{3533}$mod 11413=5761 and sends it to Bob.**
- **Bob computes b^{-1}mod Φ(n)=6597 and decrypts using 5761^{6597} mod 11413=9726**

Efficient Exponentiation

- **Compute x^c efficiently mod n.**
- **Express c as follows:** $c = \sum_{i=0}^{\ell-1} c_i 2^i$

SQUARE-AND-MULTIPLY(x, c, n)

$z \leftarrow 1$
for $i \leftarrow \ell - 1$ **downto** 0
do $\begin{cases} z \leftarrow z^2 \bmod n \\ \textbf{if } c_i = 1 \\ \quad \textbf{then } z \leftarrow (z \times x) \bmod n \end{cases}$
return (z)

Choosing the parameters of RSA

RSA PARAMETER GENERATION	
1.	Generate two large primes, p and q, such that $p \neq q$
2.	$n \leftarrow pq$ and $\phi(n) \leftarrow (p-1)(q-1)$
3.	Choose a random b $(1 < b < \phi(n))$ such that $\gcd(b, \phi(n)) = 1$
4.	$a \leftarrow b^{-1} \bmod \phi(n)$
5.	The public key is (n, b) and the private key is (p, q, a).

- **n is known, but its factors are not known**
- **b is also known, so to compute a one needs the value of Φ(n), for which we need p and q**
- **It has been conjectured that breaking RSA is polynomially equivalent to factoring n. But there is no proof!**
- **Typically, value of n is 1024 bit long and the factors are also large of around 512 bits.**

Primality Testing

- **How do we say whether a given number is prime?**
- **We propose randomized algorithms, called Monte-Carlo algorithms**
- **These algorithms give an answer in time that is polynomial in $\log_2 n$, which is the number of bits required to store n.**
- **However there is a probability that the algorithm may claim that n is prime when it is not. These numbers are called pseudo-primes.**

Prime Number Theorem

- Number of primes that are less than or equal to N is given by:

$$\pi(N) \approx \frac{N}{\ln \text{ N}}$$

Hence,…

- If N is a 512 bit number, then there are around $2^{512}/\ln 2^{512} \approx 2^{512}/355$.
- So, a random 512 bit integer will be prime with probability of 1/355.
- Thus, if you choose 355 integers then there is one number which is prime
- If you choose only odd numbers the probability doubles.

Monte-Carlo Algorithm

- **Randomized algorithm, which is yes based**
  - **There is always an answer**
  - **When the answer is yes, it is correct**
  - **If the answer is no, the answer may be wrong**
- **(Error Probability=ε) => (for any instance if the answer is yes, it can say no with a probability at most ε).**
- **The probability is over all random choices of the algorithm.**

The Problem Composites

	Composites
Instance:	A positive integer $n \geq 2$.
Question:	Is n composite?

- **This is a decision problem.**
- **We will discuss the Solovay-Strassen Algorithm, which is a Monte-Carlo algorithm for Composites.**
- **Thus if it says yes, n is surely composite.**
- **However, if n is composite then it says yes with probability at least ½**

Quadratic Residue

Suppose p is an odd prime and a is an integer. a is defined to be a *quadratic residue* modulo p if $a \not\equiv 0 \pmod{p}$ and the congruence $y^2 \equiv a \pmod{p}$ has a solution $y \in \mathbb{Z}_p$. a is defined to be a *quadratic non-residue* modulo p if $a \not\equiv 0 \pmod{p}$ and a is not a quadratic residue modulo p.

- **There are exactly (p-1)/2 QR (Quadratic Residues)**

Example

- Z_{11}
  - $1^2=1$
  - $2^2=4$
  - $3^2=9$
  - $4^2=5$
  - $5^2=3$
  - $6^2=3$
  - $7^2=5$
  - $8^2=9$
  - $9^2=4$
  - $10^2=1$

Note, that the QR forms a palindrome

There are exactly (11-1)/2=5 QRs.

Generalization

How many solutions are there to $x^2 \equiv a(\text{mod } p)$
for odd positive prime p?
If, $y^2 \equiv a(\text{mod } p), y \in Z_p^*$
then $(-y)^2 \equiv a(\text{mod } p)$
Note, $y \equiv -y(\text{mod } p)$, as p is odd
Thus, the quadratic congruence:
$x^2 - a \equiv 0(\text{mod } p)$
can be factored into
$(x - y)(x + y) \equiv 0(\text{mod } p)$
Since, p is prime, $p \mid (x - y)$ or $p \mid (x + y)$
Thus, $x \equiv \pm y(\text{mod } p)$
Thus, there are exactly two solutions of the congruence.

The QR Problem

	Quadratic Residues
Instance:	An odd prime p, and an integer a.
Question:	Is a a quadratic residue modulo p?

- **We have a polynomial time deterministic algorithm to solve this decision problem.**

Euler comes to the rescue again

(Euler's Criterion) *Let p be an odd prime. Then a is a quadratic residue modulo p if and only if*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

- **The time complexity of this check is O(log p)[3] by applying square and multiply method to raise an element to a power.**
- **Note that if** $a^{(p-1)/2} \equiv -1 \pmod{p}$ **then a is a non-quadratic residue.**

Legendre Symbol

Suppose p is an odd prime. For any integer a, define the *Legendre symbol* $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Suppose p is an odd prime. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Jacobi Symbol

Suppose n is an odd positive integer, and the prime power factorization of n is

$$n = \prod_{i=1}^{k} p_i^{e_i}.$$

Let a be an integer. The *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined to be

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Example

- **Compute** $\left(\frac{6278}{9975}\right)$
- **Note 9975=3x5^{2}x7x19**

$$\left(\frac{6278}{9975}\right) = \left(\frac{6278}{3}\right)\left(\frac{6278}{5}\right)^2\left(\frac{6278}{7}\right)\left(\frac{6278}{19}\right)$$

$$= \left(\frac{2}{3}\right)\left(\frac{3}{5}\right)^2\left(\frac{6}{7}\right)\left(\frac{8}{19}\right)$$

$$= (-1)(-1)^2(-1)(-1) = -1$$

References

- **D. Stinson, Cryptography: Theory and Practice, Chapman & Hall/CRC**

Next Days Topic

- **Primality Testing**