
NELCO
Sweet
Chocolate
150 g
my FAVOURITE

sooraj551729@gmail.com +91-9400635788

INDEX

Name SOORAJ · S · Sub. Cryptography (A5)

Std ______ Div. ______ Roll No ______

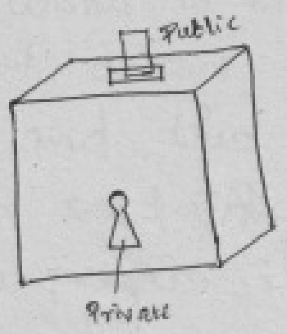
S. No	Topic	Page No	Date	Grade/ Marks	Signature
	QUANTUM COMPUTATION				
	& QUANTUM INFORMATION				
	- Nielsen & Chuang.				

Public key cryptography and the RSA cryptosystem

Cryptography is the art of enabling 2 parties to communicate in private.

Effective cryptosystems make it easy for parties who wish to communicate to do so, but make it very difficult for 3rd parties to 'eavedrop' on the contents of the conversation.

Cryptosystem Imp. Ex: Public key cryptosystems.



Basic Idea

Suppose Alice wishes to receive messages using a public key cryptosystem. She must 1st generate 2 cryptographic keys, one a public key P and the other a secret key S.

The exact nature of these keys depends on the details of the cryptosystem being used.

Once Alice has generated her keys, she publishes the public key so that anybody can obtain access to the key.

Now,

Suppose Bob wishes to send Alice a private message. He 1st obtains a copy to Alice's public key P, and then encrypts the message he wishes to send Alice, using Alice's public key to perform the encryption.

Exactly how the encryption transformation is performed depends on the details of the cryptosystem in use.

In order to be secure against eavesdropping the encryption stage needs to be very difficult to reverse, even making use of the public key used to encrypt the message in the 1st place.

⟹ What you can put in, you can't take back out, even if you have the key to the trap door.

Since the public key and the encoded message is the only information available to an eavesdropper, it won't be possible for the eavesdropper to recover the message.

Alice has an additional piece of information not available to an eavesdropper, the secret key S. The secret key determines a second transformation, on the encrypted message. This transformation is known as decryption, and is inverse to encryption allowing Alice to recover the original message.

Public key cryptosystem example

— RSA cryptosystem

Start out with the message itself, symbolized by M, which is to be "encrypted". There are 4 procedures that are specific and essential to a public-key cryptosystem:

(a) Deciphering an enciphered message gives you the original message.

$$D(E(M)) = M$$

(b) Reversing the procedures still returns M:

$$E(D(M)) = M$$

(c) E and D are easy to compute

(d) The publicity of E does not compromise the secrecy of D, i.e., you can't easily figure out D from E.

RSA cryptosystem - Math

Lets represent M by an integer between 0 and n-1. If the message is too long, sparse it up and encrypt separately.

Let e,d,n be +ve integers with (e,n) as the encryption key, (d,n) the decryption key, with n = pq.

We encrypt the message by raising it to the e^{th} power modulo n to obtain C, the ciphertext. We then decrypt C by raising it to the d^{th} power modulo n to obtain M again.

$$C \equiv E(M) \equiv M^e \pmod{n}$$

$$M \equiv D(C) \equiv C^d \pmod{n}$$

- First, choose 2 random large primes p and q, and multiply to produce $n = pq$.

Although n is public, it will not reveal p and q since it is essentially impossible to factor them from n, and therefore will assure that d is practically impossible to derive from e.

We pick d to be a random large integer, which must be coprime to $(p-1)\cdot(q-1)$

i.e., $\gcd(d, (p-1)(q-1)) = 1$

We'll want to compute e from d, p and q. where e is the multiplicative inverse of d. i.e.,

$$e \cdot d = 1 \pmod{\phi(n)}$$

where $\phi(n)$ is the Euler totient function $\phi(n)$ whose output is the # of +ve integers less than n which are coprime to n.

For primes p, $\phi(p) = p-1$

and $\phi(ab) = \phi(a)\phi(b)$

$\therefore$

$$\begin{aligned}\phi(n) = \phi(pq) &= \phi(p)\cdot\phi(q)\\ &= (p-1)(q-1)\\ &= n-(p+q)+1\end{aligned}$$

$e \cdot d \equiv 1 \pmod{\phi(n)}$

$\Longrightarrow \quad e \cdot d = k\phi(n) + 1$ for some $k \in \mathbb{Z}$

By the laws of modular arithmetic, the multiplicative inverse of a modulo m exists iff a and m are coprime.

Since d and $\phi(n)$ are coprime, d has a multiplicative inverse e in the ring of integers modulo $\phi(n)$.

Since,

$$D(E(M)) = (E(M))^d = (M^e)^d \pmod{n} = M^{e \cdot d} \pmod{n}$$

$$E(D(M)) = (D(M))^e = (M^d)^e \pmod{n} = M^{e \cdot d} \pmod{n}$$

and also since $e \cdot d = k \cdot \phi(n) + 1$

$M^{e \cdot d} = M^{k\phi(n)+1} \pmod{n}$

We want this to be equal to M.

Euler's theorem $\Rightarrow$

For any integer M coprime to n, we have $M^{\phi(n)} \equiv 1 \pmod{n}$

$0 \le M < n$ where $n = pq$, we know that M would not be coprime to n iff M was either p or q, of the integers in that interval.

$\therefore$ The chances of M happening to be p or q are on the same order of magnitude as $2/n$.

i.e., M is almost definitely relatively prime to n.

$\Longrightarrow M^{\phi(n)} \equiv 1 \pmod{n}$ holds.

$$M^{e\cdot d} \equiv M^{k\phi(n)+1} \equiv \left(M^{\phi(n)}\right)^{k} M \equiv 1^{k} M \pmod{n} = M$$

Alice makes known 2 numbers, n and e which she has selected carefully. Then Bob can use these numbers to encode a message and send it to Alice. A 3rd party Oscar has free access to n, e and the encoded message. It should be essentially impossible for Oscar to decode the message But Alice can decode the message easily because she knows a secret.

Briefly

The RSA cryptosystem is an example of a public key system — everyone can know the encryption key but it is computationally infeasible for an unauthorized person to deduce the corresponding description key.

The RSA modulus n is a positive integer which equals the product of 2 distinct prime numbers p and q:

RSA modulus: $n = pq$

Also needed is an encoding exponent e. such that $\gcd(e,(p-1)(q-1)) = 1$

Typically, e is chosen first, and then Alice picks p and q so that the condition $\gcd(e,(p-1)(q-1))=1$ holds.

Encoding: $C \equiv M^{e} \pmod{n}$

To decode the message C, Alice uses the values p and q. After picking n and e, she computes d by:

Decoding Exponent:
$$d = e^{-1} \pmod{\phi(n)}$$
$$= e^{-1} \pmod{\phi(pq)}$$
$$= e^{-1} \pmod{(p-1)(q-1)}$$

such that $ed = 1 \pmod{\phi(n)}$

This inverse is the same as is used in the Affine and Hill ciphers, and it can be computed efficiently by the extended Euclidean Algorithm.

Alice then decodes the message by computing:

Decoding: $M = C^{d} \pmod{n}$

We now see Alice's secret: she knows p and q i.e., she knows how to factor n.

In practice, she starts with a large primes p and q, and multiplies them together to get n. For RSA to be secure, n has to be hard to factor or else Oscar can determine p and q, in which case he can also compute d and decode messages.

Ex:-

Suppose the encoding exponent is $e = 17$ and the Alice chooses $p = 5$ and $q = 11$, so $n = pq = 55$.

Note that, $\gcd(e, (p-1)(q-1)) = \gcd(17, 40) = 1$.

Now,
suppose Bob wants to encode the "message" $M = 37$. He computes,

$$C = M^e \pmod{n} = 37^{17} \pmod{55} = 27$$

Alice also computes $d = e^{-1} \pmod{(5-1)(11-1)}$

$$= 17^{-1} \pmod{40} = 33$$

$ed \pmod{(p-1)(q-1)} = 17 * 33 \pmod{4 \times 10} = 561 \pmod{40} = 1$

Then she can decode the message:

$$C^d \pmod{n} = 27^{33} \pmod{55} = 37$$

Diffie-Hellman key Exchange

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

Ex:- The Enigma machine.

The common charakteristics of symmetic ciphers is that the two communicating parties Alice and Bob hold the same private key that is used for both encryption and decryption of the message.

How can Alice & Bob agree on a specific secret key when communicating through a completely insecure channel?

The Discrete Logarithm problem (DLP)

The function logarithm is represented as,

$$y = \log_b(x)$$

where x, y and b are related by,

$$x = b^y.$$

where b is known as the base of the logarithm.

The logarithm problem is the problem of finding y knowing b and x.

This is straight forward to do if we work in the algebraic field of real numbers.

The logarithm problem can be reformulated when instead of working in the real number field we work on the prime modulo algebraic field.

The discrete logarithm problem (DLP):

Find y knowing x, g and p such that

$$x = g^{y} \pmod{p}$$

where p is a prime # and g is a generator of the group defined by p.

* $(\mathbb{Z}_p^*, \cdot)$ is a cyclic group.

Ex:-

$$(\mathbb{Z}_7^*, \cdot) = \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\}$$

$$= \langle 5 \rangle = \{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 4, 6, 2, 3\}$$

$$\neq \langle 2 \rangle = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4, 1, 2, 4\}$$

$$= \{1, 2, 4\}.$$

Why do we use a generator 'g' instead of any number b/w 1 and p-1 ?

It's because with g we increment the search space.

i.e., any # between 1 and p-1 is a valid candidate for y, the # we are looking for. This makes the problem harder.

□ The Diffie-Hellman key exchange.

The Diffie-Hellman key exchange algorithm solves the following dilemma: Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure. Every piece of information that they exchange is observed by their adversary Eve. How is it possible for Alice and Bob to share a key without making it available to Eve?

The difficulty of the discrete logarithm problem for $\mathbb{F}_p^*$ provides a possible solution.

Algorithm

The 1st step is for Alice and Bob to agree on a large prime p and a non-zero integer g modulo p.

Alice & Bob make the values p and g public knowledge; for example, they might post the values on their websites, so Eve knows them too.

The next step is for Alice to pick a secret integer 'a' that she does not reveal to anyone, while at the same time Bob picks an integer 'b' that he keeps secret. Bob and Alice use their secret integers to compute:

$$\underbrace{A \equiv g^{a} \pmod p}_{\text{Alice computes this}} \quad \text{and} \quad \underbrace{B \equiv g^{b} \pmod p}_{\text{Bob computes this}}$$

They next exchange these computed values, Alice sends A to Bob and Bob sends B to Alice.

Note that Eve gets to see the values of A and B, since they are sent over the insecure communication channel.

Finally,

Bob and Alice again use their secret integers to compute

$$\underbrace{A' \equiv B^a \pmod{p}}_{\text{Alice computes this}} \quad \text{and} \quad \underbrace{B' \equiv A^b \pmod{p}}_{\text{Bob computes this}}$$

The values that they compute, A' and B' respectively, are the same, since

$$A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B' \pmod{p}$$

This common value is their exchanged key.

Example

Alice & Bob agree to use the prime $p = 941$ and the primitive root $g = 627$.

Alice uses the secret key $a = 347$ and computes, $A = 390 \equiv (627)^{347} \pmod{941}$.

Similarly, Bob chooses the secret key $b = 781$ and computes, $B = 691 \equiv (627)^{781} \pmod{941}$

Alice sends Bob the number 390 and Bob sends Alice the number 691. Both of these transmissions are done over an insecure channel, so both $A = 390$ and $B = 691$ should be considered public knowledge. The numbers $a = 347$ and $b = 781$ are not transmitted and remain secret. Then Alice & Bob are both able to compute the number

$$470 \equiv (627)^{347 \times 781} \equiv A^b \equiv B^a \pmod{941}.$$

$\therefore$ 470 is their shared secret.

Suppose that,

Eve sees this entire exchange. She can reconstitute Alice's and Bob's shared secret if she can solve either of the congruences

$$627^a \equiv 390 \pmod{941}$$

[OR] $$627^b \equiv 691 \pmod{941}$$

since then she will know one of their secret exponents. As far as is known, this is the only way for Eve to find the secret shared value without Alice's or Bob's assistance.

* Current guidelines suggest that, Alice & Bob choose a prime p having approximately 1000 bits (i.e., $p \approx 2^{1000}$) and an element g whose order is prime & approximately p/2. Then Eve will face a truly difficult task.

In general,

Eve's dilemma is this. She knows the values of A and B, so she knows the values of g^a and g^b. She also knows the values of g and p, so if she can solve the DLP, then she can find 'a' and 'b', after which it is easy for her to compute Alice and Bob's shared secret value g^{ab}.

It appears that Alice and Bob are safe provided that Eve is unable to solve the DLP, but this is not quite correct.

It is true that one method of finding Alice and Bob's shared value is to solve the DLP, but that is not the precise problem that Eve needs to solve.

The security of Alice's and Bob's shared key rests on the difficulty of the following, potentially easier, problem.

Definition: Let p be a prime # and g an integer. The Diffie-Hellman problem (DHP) is the problem of computing the values of $g^{ab} \pmod p$ from the known values of $g^{a} \pmod p$ and $g^{b} \pmod p$.