Cryptology 3rd November 2015

Lecture 12: Introduction to PKC; RSA I

Instructor: Goutam Paul *Scribe: Diptendu Chatterjee*

1 Public or Asymmetric Key Cryptography

In Symmetric or Private key Cryptography, We have seen that for message 'm', cipher text 'c', shared secret key 'k' :

i. Encryption : $c = E_k(m)$.

ii. Decryption : $m = D_k(c)$.

iii. $m = D_k(E_k(m))$.

But in Asymmetric or Public Key Cryptography, every user has one public encryption key (e) and one private decryption key (d). So here for message 'm', cipher text 'c' :

i. First receiver publishes his encryption key 'e'.

ii. Then sender sends the encrypted message as : $c = E_e(m)$.

iii. And then receiver decrypts the encrypted message as : $m = D_d(c) = D_d(E_e(m))$.

1.1 Advantages of Public Key Cryptography over Private Key Cryptography

I. The number of distinct keys required for private key cryptography is of the order of 'n^2' and that of the public key Cryptography is of the order 'n' when the number of user is 'n'. So, public key cryptography will need less storage space.

II. Unlike private key cryptography, the sender and receiver do not need any prior secret communication for key sharing. Here the receiver publishes his encryption key for everyone.

III. In most of the public key cryptosystem the security is based on "hard" number theoretic problems.

1.2 Disadvantages of Public Key Cryptography over Private Key Cryptography

I. Algorithms involved in public key cryptosystem are much slower compared to those of the private key cryptosystem.

So in practice we use advantages of both private and public key cryptography. In that case public key cryptographic method is used for priliminary key sharing as for that no prior secret communication is required. Then the message is encrypted using the key and communicated using private key cryptosystem as it is faster compared to public key cryptosystem.

1.3 RSA Cryptosystem

1.3.1 Key Setup

Key setup is initiated by the receiver. Following are the steps:

I. Take two large prime numbers. Say 'p', 'q'.

II. Compute $N = p \times q$.

III. Compute $\Phi(N) = \Phi(p \times \mathrm{q}) = (p-1) \times (q-1)$. Where Φ is Euler's Totient Function.

IV. Choose an integer 'e' coprime to $\Phi(N)$.

V. Find $d = e^{-1} \bmod \Phi(N)$.

VI. Publish (N, e) as public key.

VII. Keep $d, p, q, \Phi(N)$ as secret.

1.3.2 Encryption

Encryption is done by sender using the following steps:

i. Get the public key pair (N, e) published by receiver.

ii. Encrypt the message 'm' (i.e. the key for private key cryptosystem) as 'c', where $c = m^e \bmod N$ and send it to the receiver.

1.3.3 Decryption

Decryption is done by receiver using the following steps:

i. Get the encrypted message 'c' sent by sender.

ii. Decrypt the cipher text 'c' to 'm'(i.e. the key for private key cryptosystem), where $m = c^d \bmod N$.

1.4 Proof of Correctness of RSA Algorithm

To prove the correctness of RSA algorithm, we have to show $(m^e)^d \bmod N = m \bmod N$.

1.5 Proof

$(m^e)^d \bmod N = m^{ed} \bmod N = m^{t\Phi(N)+1} \bmod N = m \bmod N$.
Where t is some integer. [As $d = e^{-1} \bmod \Phi(N)$]
There can be different cases as follows:

1.5.1 Case:1

$m \in Z_N^*$, where Z_N^* is the set of all integers less than N and coprime to N.
Here, By Euler's Theorem $m^{\Phi(N)}$=1 mod N.
So,$m^{t\Phi(N)}$=1 mod N.
And $m^{t\Phi(N)+1}$= m mod N.

1.5.2 Case:2

$m \notin Z_N^*$.

1.5.3 Case:2(a)

$m = 0$ mod p and $m = 0$ mod q.
So, $p \mid m^{ed} - m$ and $q \mid m^{ed} - m$.
$\Rightarrow pq \mid m^{ed} - m$
$\Rightarrow m^{ed} \equiv m$ mod N.

1.5.4 Case:2(b)

$m = 0$ mod p and $m \neq 0$ mod q.
$\Rightarrow m^{ed} - m = 0$ mod p.
Now,
m^{ed} mod q
$= m^{t\Phi(N)}.m$ mod q
$= m^{(q-1)(p-1)t}.m$ mod q
$= (m^{(q-1)})^{(p-1)t}.m$ mod q
$= m$ mod q. [By Fermat's Little Theorem $m^{q-1} \equiv 1$ mod q, where q is a prime and $q \nmid m$].
$\Rightarrow m^{ed} - m = 0$ mod q
$\Rightarrow m^{ed} - m = 0$ mod pq
$\Rightarrow m^{ed} - m = 0$ mod N.

1.5.5 Case:2(c)

$m = 0$ mod q and $m \neq 0$ mod p. In this case, the proof is similar to that of Case:2(b) with only interchange of p and q.