

Network Security - CSE 508 - Fall 09

Faculty - Rob Johnson

Monday October 12, 2009

1 Public Key Cryptography

1.1 Key Agreement or Exchange - Requirements

- Secrecy - In Public Key Cryptography, secrecy is not required
- Integrity and Availability are still requirements we should try to achieve though.

1.2 Safe Crypt - an instance of Public key cryptography

- Bob sends Alice a “safe” to send a message in.
- Alice sends $E_k(m)$ to Bob.
- This ensures that Bob, the safe sender is the recipient.
- This method does not authenticate Alice.

2 Introduction to RSA and Number Theory

- Bob picks two large prime nos, p and q .
- Let $N = p * q$.
- Pick e, d such that $ed = 1 \text{ mod } (p-1)(q-1)$ or we can also say $ed = X(p-1)(q-1) + 1$ where e, d are the encryption and decryption keys respectively.
- Bob sends Alice (e, N) so that Alice can encrypt the message as $c = m^e \text{ mod } N$ and send it to Bob.
- Bob decrypts the ciphertext to the plaintext using the decryption key, $m = c^d \text{ mod } N$.

2.1 Proof for RSA

- $\rightarrow c^d \equiv (m^e)^d \pmod{N}$
 $\rightarrow c^d \equiv (m^{ed}) \pmod{N}$
 $\rightarrow c^d \equiv (m^{X(p-1)(q-1)+1}) \pmod{N}$
We know from Euler's Theorem that $m^{(p-1)(q-1)} \equiv 1 \pmod{N}$
Hence $\rightarrow (1 \pmod{N} * m) \pmod{N}$
 $m \pmod{N}$

2.2 Attacking RSA

- One of the common ways of attacking RSA is to attempt to factorise the product of the two large primes $N = p * q$.
- The best known factoring algorithm is the Generalised Number Field Sieve (G.N.F.S.).
- If N is n bits long, then GNFS runs in $O(e^{2n^{1/3}(\log n)^{2/3}})$
- For eg., when $n = 640$ bits, it takes 8 months and 80 optorons.
- For eg., when $n = 2048$ bits, it takes 8 million times harder.

2.3 Finding large prime numbers

- Fact (Prime Number Theorem) - The no. of prime nos. $\leq x$ is $(x/\ln x)$.
- For eg., there are about $2^{1024}/(\ln 2^{1024})$ primes $\leq 2^{1024}$, which is almost equal to $2^{1024}/700$ approximately.
- To find a large prime, $1 < m < N$,
 1. Pick a random no., $X \leq 2^{1024}$.
 2. Test if it is prime.
 3. Repeat until success.
- The logical next step would be to figure out how to efficiently test for a prime no.

2.4 Chosen CipherText attacks

- Mallory has a ciphertext, c .
- Mallory computes $c' = 2^e * c \pmod{N}$
- Bob decrypts $m' = 2^{ed} * c^d \pmod{N}$
- $\leftarrow 2^m \pmod{N}$
- Mallory can do the following to get the plaintext, $m = 2^{-1} * 2 * m \equiv m \pmod{N}$

2.5 Basic Number Theory

- $Z/NZ = \{0, 1, 2, 3, 4 \dots (N - 1)\}$
- If a, b belong to Z/NZ , $a + b = (a + b) \bmod N$ and $a * b = (a * b) \bmod N$ where $+, *$ are operations on the set.
- Fact: These operations are commutative, distributive, associative and $0, 1$ exists.
- Fact: Negatives exist and inverses sometimes exist.

2.6 Greatest Common Divisor GCD

- We define the longest common divisor as $gcd(a, b)$
- Fact: $gcd(a, b) = 1$, they are relatively prime.
- If $gcd(a, b) = X$, X is the smallest positive integer of the form $sa + tb$ where $s, t \in Z$.
- Proof:
 - Suppose $d|a$ and $d|b$, then $d|(sa + tb)$.
 - So, $gcd(a, b)|(sa + tb)$
 - Hence $gcd(a, b)|X$