CS3200: Computer Networks

Lecture 35

IIT Palakkad

10 Nov, 2019

Public-Key Algorithms

- Distributing the keys has always been the weakest link in most cryptosystems.
- Keys had to be protected from theft, but they also had to be distributed, so they could not be locked in a bank vault.
- In 1976, two researchers at Stanford University, Diffie and Hellman (1976), proposed a radically new kind of cryptosystem, one in which the encryption and decryption keys were so different that the decryption key could not feasibly be derived from the encryption key

Public-Key Algorithms

In their proposal, the (keyed) encryption algorithm, E, and the (keyed) decryption algorithm, D, had to meet three requirements.

- $D(E(P)) = P$
- It is exceedingly difficult to deduce D from E.
- E cannot be broken by a chosen plaintext attack.

Public-key cryptography requires each user to have two keys: **a public key**, used by the entire world for encrypting messages to be sent to that user, and **a private key**, which the user needs for decrypting messages.

RSA

- One good method was discovered by a group at M.I.T. (Rivest et al., 1978). It is known by the initials of the three discoverers (Rivest, Shamir, Adleman): **RSA**
- It has survived all attempts to break it for more than 30 years and is considered very strong.
- Its major disadvantage is that it requires keys of at least 1024 bits for good security (versus 128 bits for symmetric-key algorithms), which makes it quite slow.

RSA

The RSA method is based on some principles from number theory. We will now summarize how to use the method.

1. Choose two large primes, p and q (typically 1024 bits).
2. Compute $n = p \times q$ and $z = (p-1) \times (q-1)$.
3. Choose a number relatively prime to z and call it d.
4. Find e such that $e \times d = 1 \mod z$.

RSA

- To encrypt a message, P, compute $C = P^e \mod n$.
- To decrypt C, compute $P = C^d \mod n$.
- The public key consists of the pair (e, n) and the private key consists of (d, n).