Foundations of Computer Security

Lecture 49: Public Key Encryption II

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

RSA Algorithm

The **Rivest-Shamir-Adelman (RSA)** algorithm relies on the difficulty of factoring large numbers.

Two keys, e and d, are used for encryption and decryption. The algorithm is such that:

$$\{\{P\}_d\}_e = P = \{\{P\}_e\}_d.$$

A plaintext block P is encrypted as $(P^e \bmod n)$. d is chosen so that:

$$(P^e)^d \mod n = P.$$

An interceptor would have to factor P^e to recover the plaintext. The legitimate receiver knows d and merely computes $(P^e)^d \bmod n = P$, which is much easier.

Other Public Key Algorithms

A public key system can be based on any one-way function. A rich source is the set of NP-complete problems. These are infeasible to solve, but a solution can be checked in polynomial time.

Merkle and Hellman proposed a public key system based on the *knapsack problem*: given a set of integers and a target sum, find a subset of the integers that sum to the target.

The algorithm is theoretically very secure, but has practical weaknesses.

Authentication with Public Keys

Assume K_a is A's public key. Suppose B sends the following message to A: $\{M\}_{K_a}$. *What assurances does A have?*

1. No-one intercepting the message could read it. *Why?*
2. He can't be sure it actually came from B. *Why not?*

Thus, encryption with the public key is a *privacy* transformation, but not an *authenticity* transformation.

Authentication with Public Keys

Using RSA, B send $\{M\}_{K_b^{-1}}$ to A. If A can decrypt it using K_b, *what assurance is gained?*

1. A is sure it originated with B. *Why?*
2. But, someone intercepting the message might read it. *Why?*

Thus, encryption with the private key is an *authenticity* transformation, not a *privacy* transformation.

Note this only works in RSA, because:

$$\{\{P\}_d\}_e = P = \{\{P\}_e\}_d.$$

In other public key systems, you typically need two pairs of keys: one pair for privacy and the other pair for "signing" (authenticity).

Lessons

- RSA is the most widely used public key cryptosystem.
- RSA is symmetric in the use of keys; most public key schemes are not.
- A public key encryption can be used for authenticity or for privacy but not both at once.

Next lecture: Cryptographic Hash Functions