Foundations of Computer Security

Lecture 48: Public Key Encryption

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

Public Key Encryption

In 1976, Whitfield Diffie and Martin Hellman proposed *public key encryption* (asymmetric encryption) in which different keys are used for encryption and decryption.

In 1997, it was disclosed that asymmetric key algorithms had been developed in the early 1970's by the British Government's Communication Headquarters (GCHQ). They referred to the technique as *non-secret encryption*.

Public Key Encryption

Use a publicly disclosed key to encrypt and a secret key to decrypt.

The requisite relationship is:

$$P = \{\{P\}_{K_{pub}}\}_{K_{priv}}.$$

We'll denote the public key for principal A by K_a and the private key will be denoted K_a^{-1}.

Public Key Systems

Also, for *some* public key systems, RSA in particular, encryption and decryption commute and either key can be used in either function. That is:

$$\{\{P\}_K\}_{K^{-1}} = P = \{\{P\}_{K^{-1}}\}_K.$$

This is crucial in some uses of RSA. *But is not true for most public key cryptosystems.*

Public Key Systems

The basis of any public key system is the identification of a *one-way function*: easily computed, but difficult to invert without additional information.

Example: It is easy to multiply two large primes p_1 and p_2. However, it is very difficult to factor $p_1 p_2$ to recover p_1 and p_2. But, given $p_1 p_2$ and either of p_1 or p_2, it is straightforward to recover the other, simply by dividing.

Efficiency of Encryption

Public key systems largely solve the key distribution problem. *Why?*

A public key encryption *may take 10,000 times as long* to perform as a symmetric encryption; the computation depends on more complex operations, not on simple bit-wise operations.

Symmetric encryption remains the work horse of commercial cryptography, with asymmetric encryption playing some important special functions.

Lessons

- Devising an asymmetric encryption algorithm depends on identifying a one-way function, easy to compute but hard to invert.
- Public key systems largely solve the key distribution problem.
- Asymmetric algorithms are generally much less efficient than symmetric algorithms.

Next lecture: Public Key Encryption II