Foundations of Computer Security

Lecture 38: Cryptography II

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

Some Terminology

Encryption and decryption are functions which transform one text into another. In functional notation:

$$C = E(P) \quad \text{and} \quad P = D(C)$$

where C denotes ciphertext, E is the encryption rule, D is the decryption rule, P is the plaintext. In this case, we also have:

$$P = D(E(P))$$

It is obviously important to be able to recover the original message from the ciphertext.

Keyed Algorithms

Often the encryption and decryption algorithms use a *key* K. The key selects a specific algorithm from the family of algorithms defined by E.

We write this dependence as:

$$C = E(P, K_E) \quad \text{and} \quad P = D(C, K_D)$$

If $K_E = K_D$, then the algorithm is called *symmetric*. If not, then it is called *asymmetric*. In general,

$$P = D(E(P, K_E), K_D)$$

An algorithm that does not use a key is called a *keyless cipher*.

Some Notation

Often the notation $E(P, K)$ and $D(C, K)$ becomes cumbersome. An alternative notation is often used, particularly in cryptographic protocols.

We'll often use $\{P\}_K$ to denote $E(P, K)$, and sometimes to denote $D(P, K)$. For example,

$$P = D(E(P, K_E), K_D) = \{\{P\}_{K_E}\}_{K_D}.$$

This is usually appropriate since, in many important commercial cryptosystems, the same algorithm is used for both encryption and decryption (i.e., the algorithm is its own inverse).

Cryptanalysis Tasks

A cryptanalyst may attempt to do any or all of the following:

- to break a single message;
- to recognize patterns in encrypted messages;
- to infer some meaning without breaking the algorithm;
- to deduce the key;
- to find weaknesses in the implementation or environment or the use of encryption;
- to find weaknesses in the algorithm, without necessarily having intercepted any messages.

Cryptanalysis Tools

The analyst works with:

- encrypted messages,
- known encryption algorithms,
- intercepted plaintext,
- data items known or suspected to be in a ciphertext message,
- mathematical and statistical tools and techniques,
- properties of languages,
- computers,
- ingenuity and luck.

Lessons

- Encryption is designed to obscure the meaning of text.
- Redundancy is the enemy of secure encryption because it provides leverage to the attacker.

Next lecture: Properties of Ciphers