Foundations of Computer Security

Lecture 45: Stream and Block Encryption

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

Stream and Block Ciphers

An important distinction in symmetric cryptographic algorithms is between *stream* and *block* ciphers.

Stream ciphers convert one symbol of plaintext directly into a symbol of ciphertext.

Block ciphers encrypt a group of plaintext symbols as one block.

Simple substitution is an example of a stream cipher. Columnar transposition is a block cipher.

Most modern symmetric encryption algorithms are block ciphers. Block sizes vary (64 bits for DES, 128 bits for AES, etc.).

Stream Encryption

Advantages:

- *Speed of transformation:* algorithms are linear in time and constant in space.
- *Low error propogation:* an error in encrypting one symbol likely will not affect subsequent symbols.

Disadvantages:

- *Low diffusion:* all information of a plaintext symbol is contained in a single ciphertext symbol.
- *Susceptibility to insertions/ modifications:* an active interceptor who breaks the algorithm might insert spurious text that looks authentic.

Block Encryption

Advantages:

- *High diffusion:* information from one plaintext symbol is diffused into several ciphertext symbols.
- *Immunity to tampering:* difficult to insert symbols without detection.

Disadvantages:

- *Slowness of encryption:* an entire block must be accumulated before encryption / decryption can begin.
- *Error propogation:* An error in one symbol may corrupt the entire block.

Malleability

An encryption algorithm is said to be *malleable* if transformations on the ciphertext produce meaningful changes in the plaintext.

That is, given a plaintext P and the corresponding ciphertext $C = E(P)$, it is possible to generate $C_1 = f(C)$ so that

$$D(C_1) = P_1 = f'(P)$$

with arbitrary, but known, functions f and f'.

Most modern block-structured ciphers are non-malleable.

Lessons

- An important distinction is between stream and block ciphers.
- Each has distinct strengths and weaknesses.
- Malleability means being able to manipulate ciphertext with predictable effects on plaintext.

Next lecture: Advanced Encryption Standard