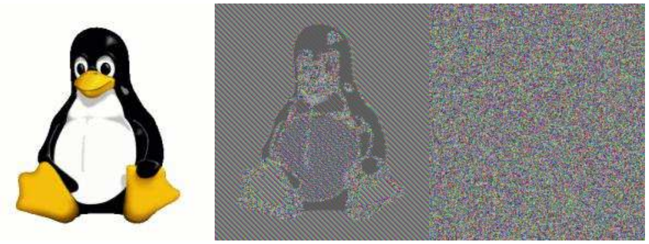
Foundations of Computer Security

Lecture 47: Modes of Usage

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

Modes of Usage: ECB

The simplest way of using a block cipher like AES is to encrypt (with the same key) each block in the plaintext. This is a *block encryption mode* called “Electronic Code Book” (ECB).



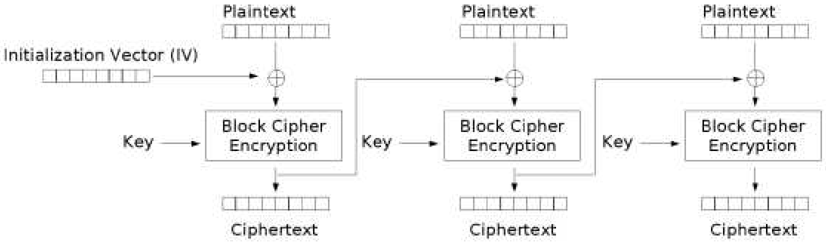
Original With ECB Another Mode

Identical blocks in the plaintext yield identical blocks in the ciphertext.

Modes of Usage: CBC

To solve the problem of EBC, do something to “randomize” blocks before they’re encrypted.

Cipher Block Chaining (CBC): XOR each successive plaintext block with the previous ciphertext block and then encrypt. An initialization vector IV is used as a “seed” for the process.



Cipher Block Chaining (CBC) mode encryption

CBC Vulnerabilities

Though much better than ECB, CBC still has some weaknesses.

Observed changes: An attacker able to observe changes to ciphertext over time will be able to spot the first block that changed.

Content Leak: If an attacker can find two identical ciphertext blocks, C_i and C_j, he can derive the following relation:

$$C_{i-1} \oplus C_{j-1} = P_i \oplus P_j,$$

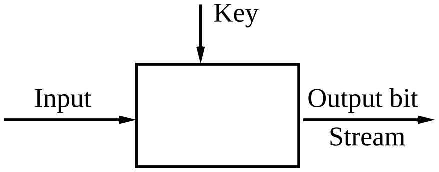
and derive information about two plaintext blocks.

Numerous other block encryption modes have been devised.

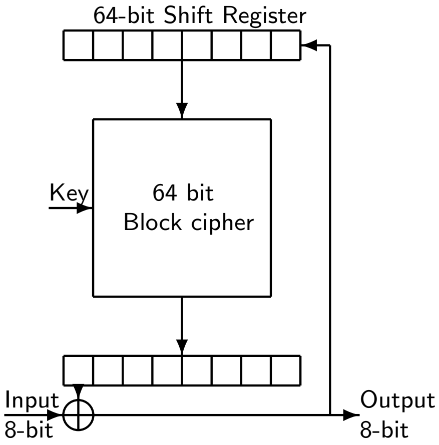
Key Stream Generation Modes

Block encryption modes (like ECB and CBC) generate ciphertext that stores the message in encrypted but recoverable form.

In *key stream generation modes* the cipher is used more as a pseudorandom number generator. The result is a key stream that can be used as in one-time pad. Decryption uses the same key stream.



Cipher Feedback Mode



In Cipher Feedback mode (CFB) each input byte is XORed with the first block of the previous output and fed back into the encryption.

Lessons

- A naive use of encryption as in Electronic Code Book leaves too much regularity in the ciphertext.
- Block encryption modes such as CBC attempt to hide this by chaining blocks together in some manner.
- Key stream generation modes use encryption algorithms to generate random appearing streams of bits in reproducible fashion.

Next lecture: Public Key Encryption