Computer Science 418

Security of Block Ciphers, Stream Ciphers, Modes of Operation

Mike Jacobson

Department of Computer Science
University of Calgary

Week 6

Outline

Security of AES

There is no mathematical proof that AES is secure

All we know is that in practice, it withstands all modern attacks.

This lecture: overview of modern attacks on block ciphers

Exhaustive Search

Set $N = |\mathcal{K}|$ (number of keys).

Simple exhaustive search (COA) — requires $|\mathcal{K}|$ encryptions

- feasible for DES — $N = 2^{56} \approx 10^{17}$ possible keys.
- infeasible for 3DES – $N = 2^{112} \approx 10^{34}$ possible key combinations.
- infeasible for AES – $N = 2^{128} \approx 10^{38}$ possible keys

Parallelism can speed up exhaustive search.

Perspective: there are approximately 10^{40} water molecules in Lake Ontario. 10^{38} is significantly bigger than the number of water molecules in Lake Louise or in the stretch of the Bow River through Calgary!

Improvement for DES

Exhaustive search for DES can be cut in half (i.e. to 2^{55} test encryptions) via the property

$$C = E_K(M) \quad \Longrightarrow \quad E_{\overline{K}}(\overline{M}) = \overline{C} \ ,$$

where $\overline{X}$ denotes the *one's complement* of a bit string X (*i.e.* each bit in X is flipped to obtain $\overline{X}$).

Mount a CPA as follows: choose two pairs $(M, C_1 = E_K(M))$ and $(\overline{M}, C_2 = E_K(\overline{M}))$. For each test key K', if

- $E_{K'}(M) = C_1$, then $K = K'$,
- $E_{K'}(M) = \overline{C}_2$, then $K = \overline{K'}$, since $E_{K'}(M) = \overline{C}_2 \Rightarrow E_{\overline{K'}}(\overline{M}) = C_2$.

Hellman's Time-memory tradeoff (1980)

KPA that shortens search time by using a lot of memory.

- The attacker knows a plaintext/ciphertext pair (M_0, C_0).
- The goal is to find the (or a) key K such that $C_0 = E_K(M_0)$.

Let $N = |\mathcal{K}|$. Cost (# of encryptions) is

Precomputation time:	N
Expected time:	$N^{2/3}$
Expected memory:	$N^{2/3}$

Large precomputation time, but improvement for individual keys

- For DES, $N^{2/3} \approx 10^{12}$ — can be done in hours or even minutes on a modern computer.

Meet-in-the-Middle Attack

KPA on double encryption.

Setup:

- Adversary has two known plaintext/ciphertexts pairs (m_1, c_1) and (m_2, c_2)
- Double-encryption, so $c_i = E_{k_1}(E_{k_2}(m_i))$ for $i = 1, 2$ and two unknown keys k_1, k_2.

Important observation: $D_{k_1}(c_i) = E_{k_2}(m_i)$ $(i = 1, 2)$.

The Atack

The adversary proceeds as follows:

1. Single-encrypt m_1 under every key K_i to compute $C_i = E_{K_i}(m_1)$ for $1 \leq i \leq N$.
2. Sort the table (or create a hash table).
3. For $j = 1$ to N do
    1. Single-decrypt c_1 under every key K_j to compute $M_j = D_{K_j}(c_1)$.
    2. Search for M_j in the table of C_i. If $M_j = C_i$ for some i, then check if $E_{K_i}(m_2) = D_{K_j}(c_2)$. If this holds, then guess $k_2 = K_i$ and $k_1 = K_j$ and quit.

Analysis

There are at most N values $E_{K_i}(m_1)$ and at most N values $D_{K_j}(c_1)$ for $1 \le i, j \le N$.

- Assuming random distribution, the chances of a match are $1/N$.
- Thus, $(N \cdot N)/N = N$ key pairs (K_i, K_j) satsify $E_{K_i}(m_1) = D_{K_j}(c_1)$.

The chances that such a key pair also satisfies $E_{K_i}(m_2) = D_{K_j}(c_2)$ are very small (paranoid users could try a third message/ciphertext pair (m_3, c_3)).

Thus, the probability of guessing correctly is very high.

Analysis, cont.

Time required:

- Step 1: N encryptions
- Step 2: sorting/hash table creation is negligible compared to Step 1
- Step 3 (a): at most N decryptions
- Step 3 (b): negligible in light of Step 2

Total: $2N$ encryptions/decryptions.

Memory: N keys and corresponding ciphertexts (the table of (C_i, K_i) pairs)

Conclusion: double encryption offers little extra protection over single encryption (hence 3DES instead of 2DES).

Linear Cryptanalysis

M. Matsui, EUROCRYPT 1993 – CCA

- Matsui actually used this method to become the first person to recover a DES key (50 days using 12 workstations).

Definition 1

A cryptosystem is *affine (linear)* if for all plaintexts M and keys K,

$$C = E_K(M) = AM + BK + H$$

where A and B are matrices and H is a vector of appropriate dimension (A, B and H are public). The system is *linear* if $H = 0$.

Note that B may or may not be square.

Example (DES)

If DES were affine, we would have the following matrix sizes:

$$A : 64 \times 64, \quad B : 64 \times 56,$$
$$K : 56 \times 1, \quad M : 64 \times 1, \quad C : 64 \times 1$$

Examples of affine linear cryptosystems are:

- the shift cipher
- the Vigenére cipher
- any transposition cipher
- the one-time pad.

Attacking Linear Cryptosystems

A cryptanalyst knowing a plaintext/ciphertext pair (M, C) can easily mount a KPA on an affine or linear system as follows:

$$\begin{aligned} BK &= C - AM - H \\ B^T BK &= B^T(C - AM - H) \\ K &= (B^T B)^{-1} B^T (C - AM - H) \end{aligned}$$

Idea of Linear Cryptanalysis

If a cryptosystem is "close to" being affine then the modified system can be broken and original system compromised after some searching.

- "close to affine" if modifying a few entries in the system (eg. in the S-boxes) makes it affine on certain plaintext/ciphertext pairs

Linear cryptanalysis attempts to "linearly approximate" non-linear cryptosystems in this way.

Every building block in DES and AES *except the S-boxes* is affine.

- S-boxes *must not* be "close" to linear (*i.e.* closely approximated by a linear function).

Differential cryptanalysis

Biham and Shamir, Journal of Cryptology, 1991 — KPA

Compares input XORs to output XORs, and traces these differences through the cipher.

Both linear and differential cryptanalysis work quite well on DES with fewer than 16 rounds.

- The first edition of Stinson's book (1995) discusses successful differential cryptanalysis attacks on 3-round and 6-round DES.
- Large-scale, parallel, brute-force attack is still the most practical attack on 16 round DES.

Requirements for full DES

Type of attack	Expected time	# of (M, C) pairs
Exhaustive search	2^{55}	none
Linear Cryptanalysis	2^{43}	2^{43} (chosen)
Differential Cryptanalysis	2^{47}	2^{47} (known)

Note: AES not affected by these attacks (by design)

Algebraic Attacks

Courtois 2001 — KPA, generates multivariate equations from from S-boxes, where the unknowns are the key bits.

- So far no threat to any modern block cipher.

Obstacle: solving multivariate equations seems to be hard in practice

Biclique Attack

Enhanced meet-in-the-middle attack using *bicliques* that map internal states to ciphertexts via subkeys.

First improved key recovery through the biclique attack on AES (Bogdanov, Khovratovich, Rechberger 2011):

AES key length	Exhaustive search	Biclique (expected)
128	2^{128}	$2^{126.1}$
192	2^{192}	$2^{189.7}$
256	2^{256}	$2^{254.4}$

These and other attacks (e.g. square attack) are successful on 8 and lower round AES.

Stream Ciphers

In contrast to block ciphers, stream ciphers don't treat incoming characters independently.

- Encryption C_i of plaintext character P_i depends on internal state of device.
- After encryption, the device changes state according to some rule.

Result: two occurrences of the same plaintext character will usually not result in the same ciphertext character.

Synchronous Stream Ciphers

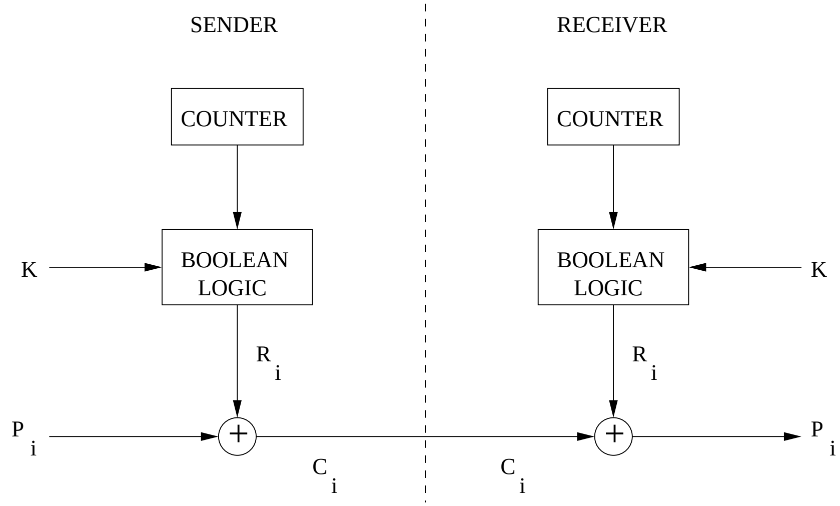
Idea:

- State depends only on the previous state, not on the input P_i.
- C_i depends only on P_i and i, not on $P_{i-1}, P_{i-2}, \ldots$
- Implemented by boolean logic that should produce a pseudo-random sequence R_i synchronized by the key (*e.g.* a shift register).

Example 2

The one-time pad can be interpreted as an SSC.

Diagram of an SSC



Block Ciphers as SSCs

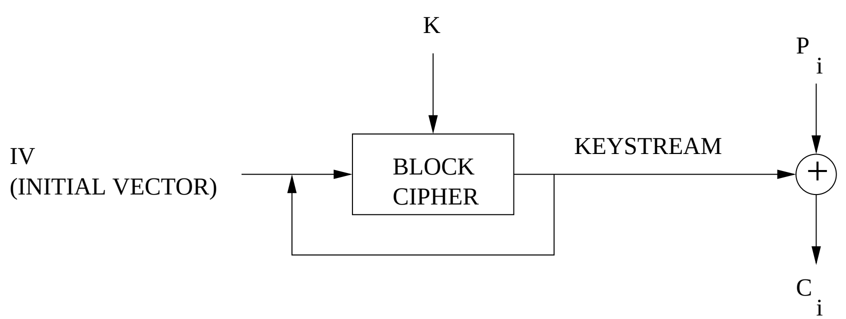
Idea:

- Send an initial key value $KS_0 = IV$ to the receiver in the clear.
- Compute $KS_i = E_K(KS_{i-1})$ and $C_i = P_i \oplus KS_i$.

Problems:

1. No error propagation
2. Loss of one character between sender and receiver destroys synchronization (no memory)

Example: Block-Cipher-based SSC

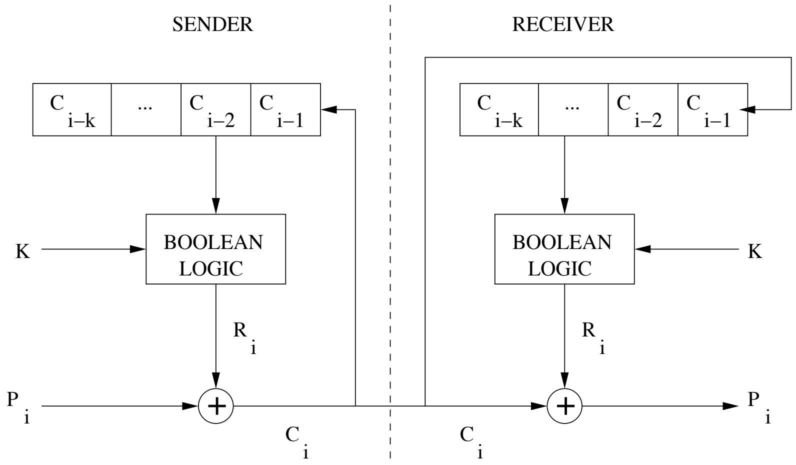


Self-Synchronizing Stream Ciphers (Self-SSC)

Idea:

- Similar to SSC, except the counter is replaced by a register containing the previous k ciphertexts.
- Self-synchronizing after k steps.
- Can also be implemented with a block cipher as above.
- Limited error propagation (k steps).

Diagram of a Self-SSC



ECB Mode

Definition 3 (Electronic code book (ECB) mode)

Blocks are encrypted sequentially, one at a time: $C_i = E_K(P_i)$, $i = 1, 2, \ldots$

A block cipher used in ECB mode is essentially a substitution cipher (with all its weaknesses).

Other Modes of Operation

To eliminate the shortcomings of ECB mode, additional modes of operation have been devised:

- Cipher Block Chaining (CBC)
- Output Feedback (OFB)
- Cipher Feedback (CFB)
- Counter (CTR)

DES Certified Modes: ECB, CBC, and CFB; standardized as part of DES standardization process.

- CTR mode arose from concerns with CBC; standardized for AES.

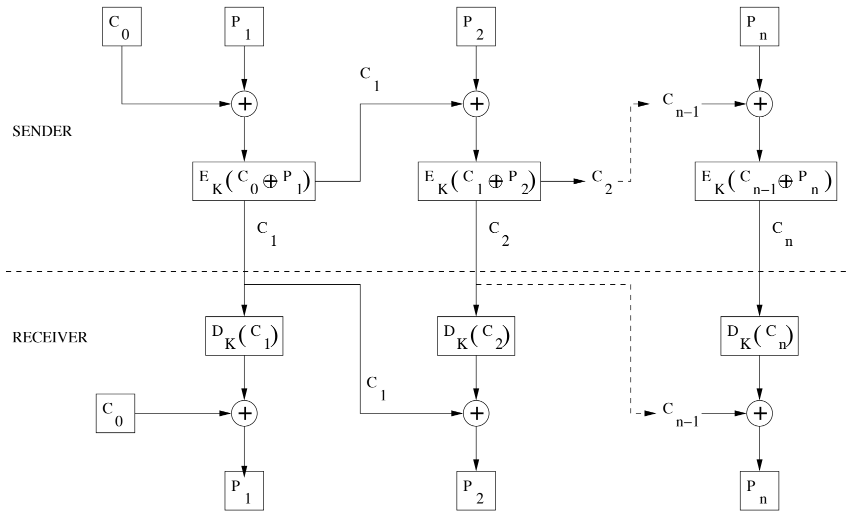
Cipher Block Chaining (CBC) Mode

Send initial *random* block $C_0 = IV$ (e.g. a simple plaintext encrypted in ECB mode, such as $C_0 = E_K(00\cdots000)$)

Encryption: $C_i = E_K(\underbrace{P_i \oplus C_{i-1}}_{\text{"Pre-Whitening"}}) \quad i = 1, 2, \ldots$

Decryption: $P_i = D_K(C_i) \oplus C_{i-1} \quad i = 1, 2, \ldots$

Diagram of CBC



Features of CBC

1. Varying *IV* encrypts the same message differently.
2. Repeated plaintexts will be encrypted differently in different repetitions.
3. Plaintext errors propogate through the rest of encryption (good for message authentication, as last ciphertext block depends on all plaintext blocks)
4. Limited error propagation in decryption: error from incorrect ciphertext modification in propagates only to the next block.

Widely used, but vulnerabilities have been discovered (eg. Vaudenay 2002 padding attack, SSL insertion attack).

Counter (CTR) Mode

A counter (CTR_i) of the same size as the cipher block size is maintained.

- Subsequent values of the counter are computed via an iterating function — the FIPS recommendation is simply $CTR_{i+1} = CTR_i + 1 \bmod 2^n$ assuming an n-bit counter.

Encryption: $C_i = E_K(CTR_i) \oplus P_i$

Decryption: $P_i = E_K(CTR_i) \oplus C_i$

Properties of CTR Mode

Counter must be unique for each plaintext block that is ever encrypted under a given key, across all messages.

- can count # of plaintext blocks encrypted under a given counter sequence — new key before exceeding 2^n blocks (n-bit blocks)

Advantages:

- only the encryption function of the block cipher is used (important for AES, in which decryption is slightly less efficient than encryption),
- the ith ciphertext block does not depend on previous ciphertext or plaintext blocks
  - allows for random-access encryption/decryption, parallelism.

Feedback Modes

The feedback modes turn a block cipher into a stream cipher

CFB (cipher feedback) mode is a self-SSC.

- Usually r cipher bits are fed back (for DES, $r = 8$ and IV is at least 48 random bits, right-justified, padded with 0's).
- Each cryptographic session requires a different IV, but these may be sent in the clear.

OFB (output feedback) is a SSC, used similarly to CFB.

Further Information

For more modes of operations as well as recommendations for other block ciphers, see the NIST Crypto Toolkit Modes of Operation page `http://csrc.nist.gov/CryptoToolkit/modes/`.