

University of Rochester
CSC290B
Introduction to Computer Security

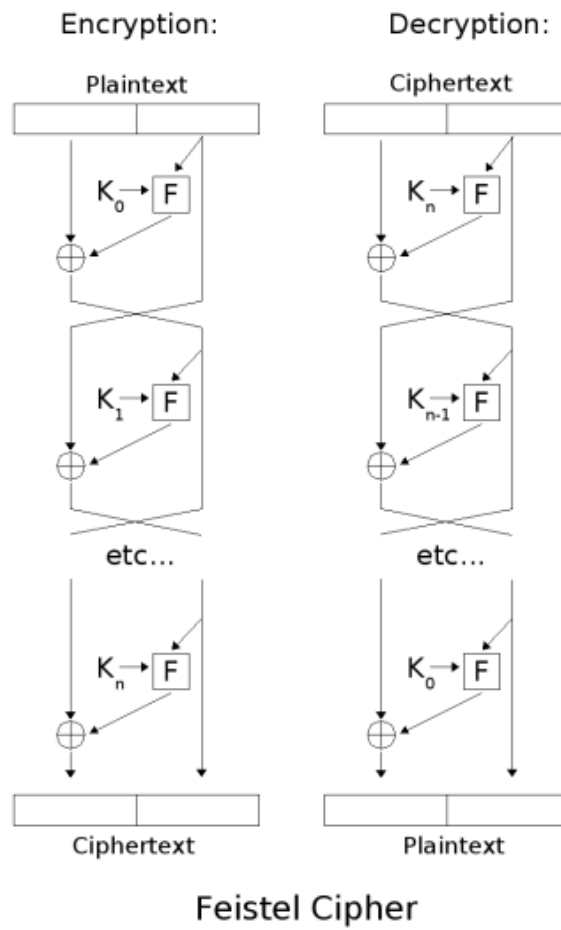
Symmetric Cryptography

March 24, 2009

Feistel Ciphers

- A method for constructing invertible keyed functions
 - Let F be the round function and let $K_0 \dots K_n$ be the subkeys for n rounds.
 - Split the plaintext block into two equal pieces, (L_0, R_0)
 - For each round, compute:
 - $L_{i+1} = R_i$
 - $R_{i+1} = L_i \oplus F(R_i, K_i)$
 - Then the ciphertext is (R_{n+1}, L_{n+1}) .
 - Decryption of a ciphertext (R_{n+1}, L_{n+1}) is accomplished by computing n rounds in opposite order:
 - $R_i = L_{i+1}$
 - $L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$
 - Then (L_0, R_0) is the plaintext again.

Feistel Cipher (diagram)

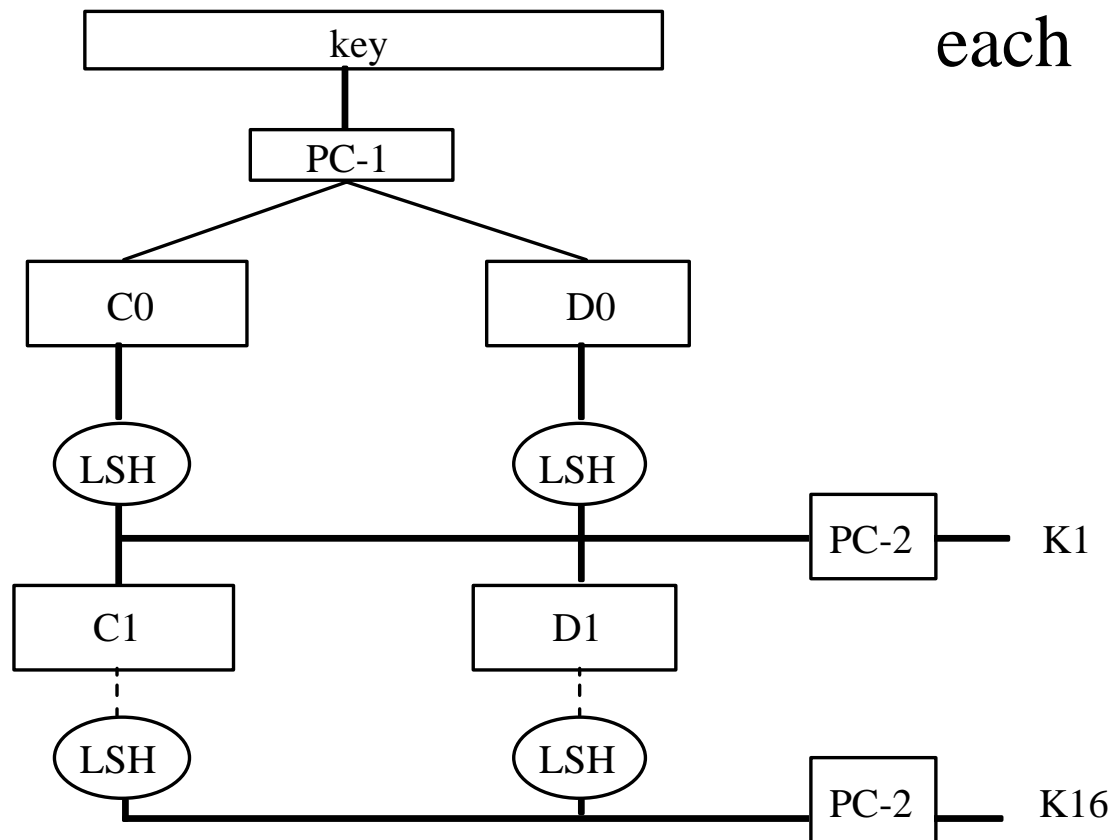


Overview of the DES

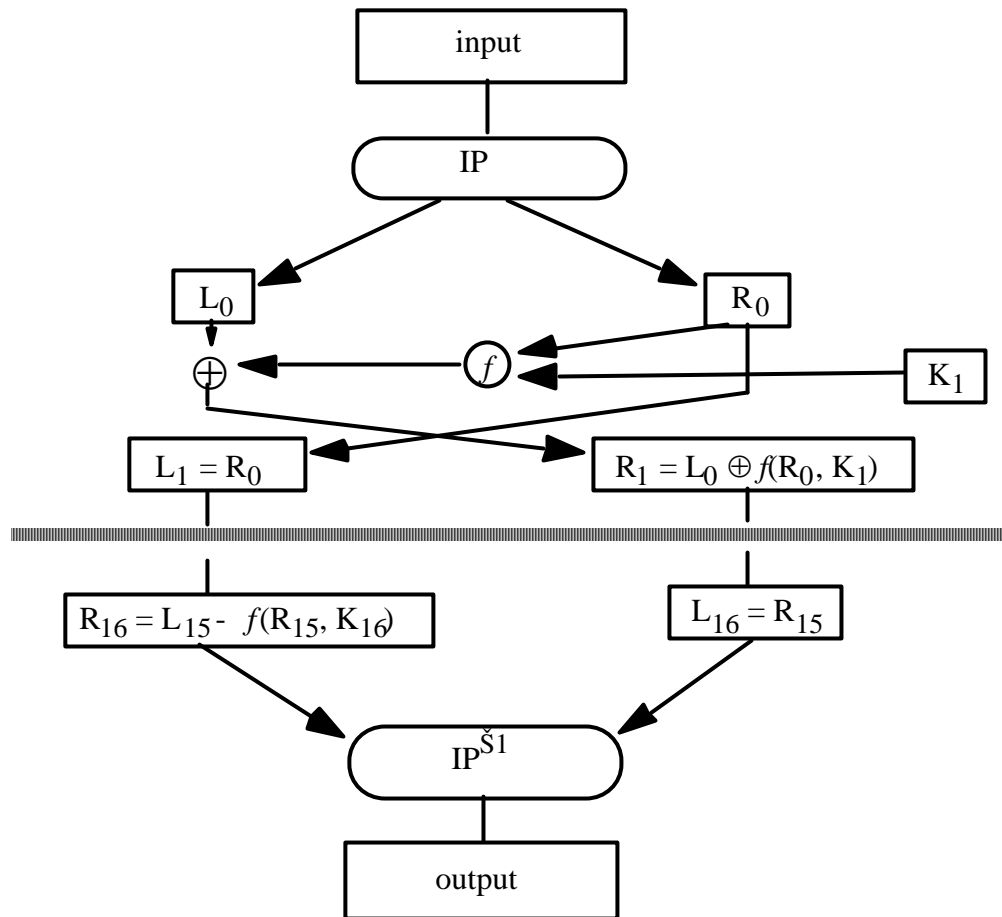
- A block cipher:
 - encrypts blocks of 64 bits using a 64 bit key
 - outputs 64 bits of ciphertext
- A product cipher
 - basic unit is the bit
 - performs both substitution and transposition (permutation) on the bits
- Cipher consists of 16 rounds (iterations) each with a round key generated from the user-supplied key

Generation of Round Keys

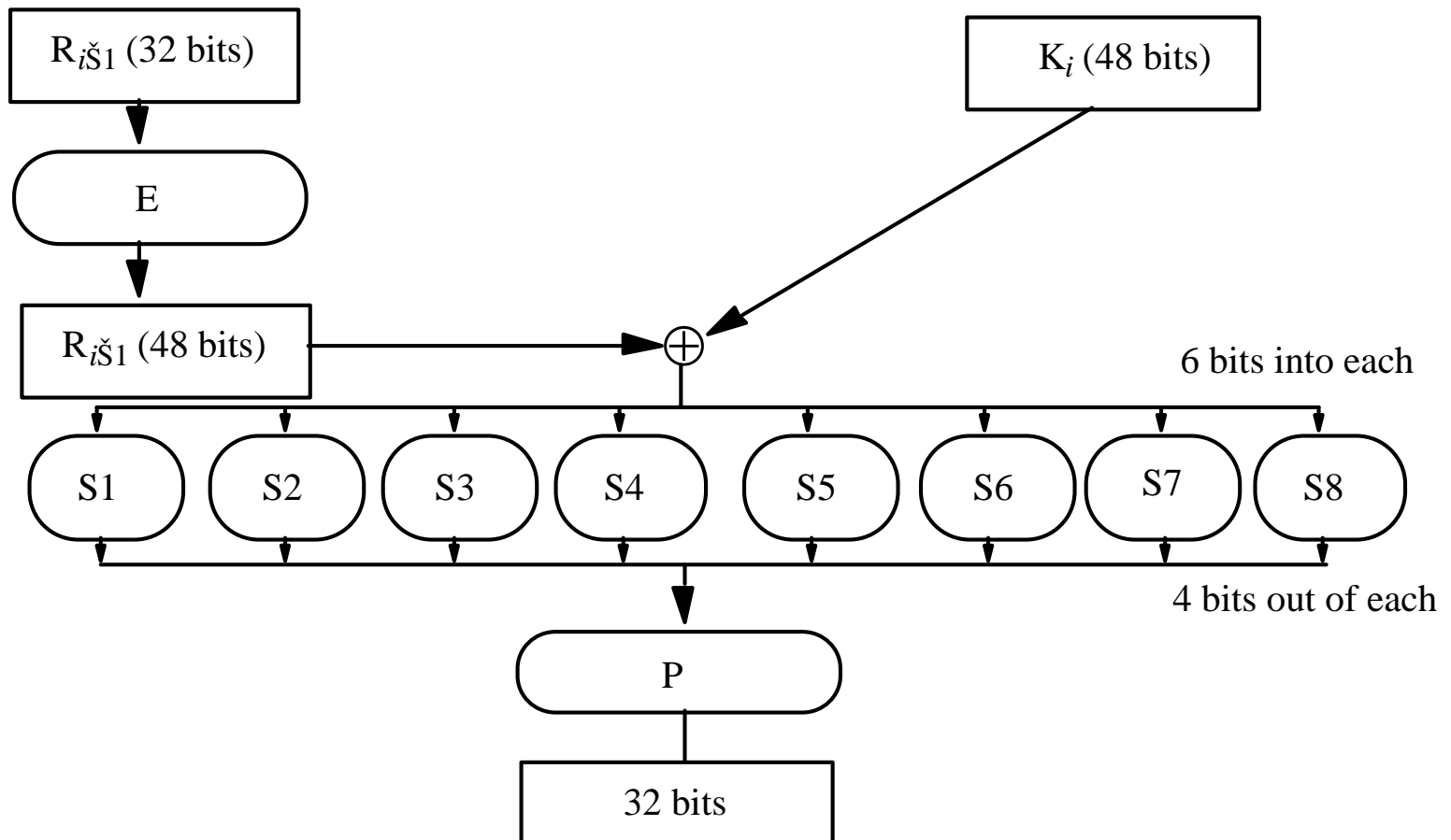
- Round keys are 48 bits each



Encipherment



The f Function



Controversy

- Considered too weak
 - Diffie, Hellman said in a few years technology would allow DES to be broken in days
 - Design using 1999 technology published
 - Design decisions not public
 - S-boxes may have backdoors

Undesirable Properties

- 4 weak keys
 - They are their own inverses
- 12 semi-weak keys
 - Each has another semi-weak key as inverse
- Complementation property
 - $\text{DES}_k(m) = c \Rightarrow \text{DES}_k(\hat{m}) = \hat{c}$
- S-boxes exhibit irregular properties
 - Distribution of odd, even numbers non-random
 - Outputs of fourth box depends on input to third box

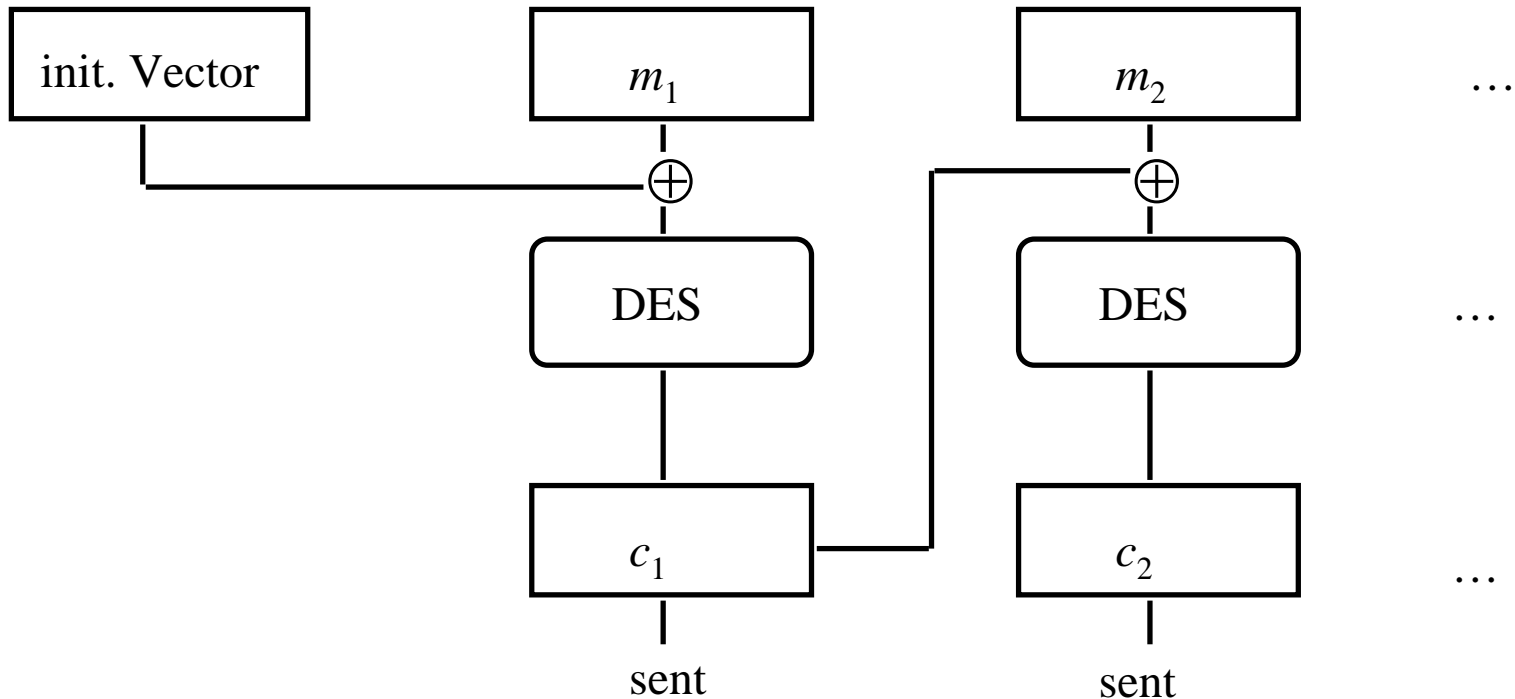
Differential Cryptanalysis

- A chosen ciphertext attack
 - Requires 2^{47} plaintext, ciphertext pairs
- Revealed several properties
 - Small changes in S-boxes reduce the number of pairs needed
 - Making every bit of the round keys independent does not impede attack
- Linear cryptanalysis improves result
 - Requires 2^{43} plaintext, ciphertext pairs

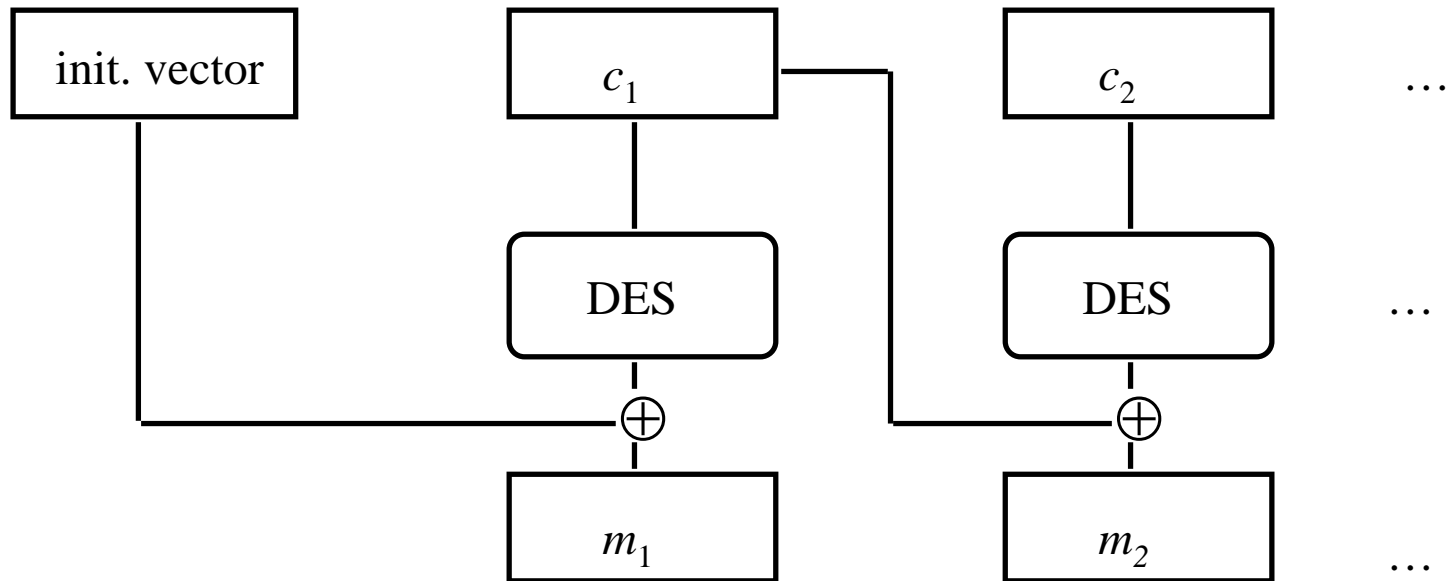
DES Modes

- Electronic Code Book Mode (ECB)
 - Encipher each block independently
- Cipher Block Chaining Mode (CBC)
 - Xor each block with previous ciphertext block
 - Requires an initialization vector for the first one
- Encrypt-Decrypt-Encrypt Mode (2 keys: k, k')
 - $c = \text{DES}_k(\text{DES}_{k'}^{-1}(\text{DES}_k(m)))$
- Encrypt-Encrypt-Encrypt Mode (3 keys: k, k', k'')
 - $c = \text{DES}_k(\text{DES}_{k'}(\text{DES}_{k''}(m)))$

CBC Mode Encryption



CBC Mode Decryption

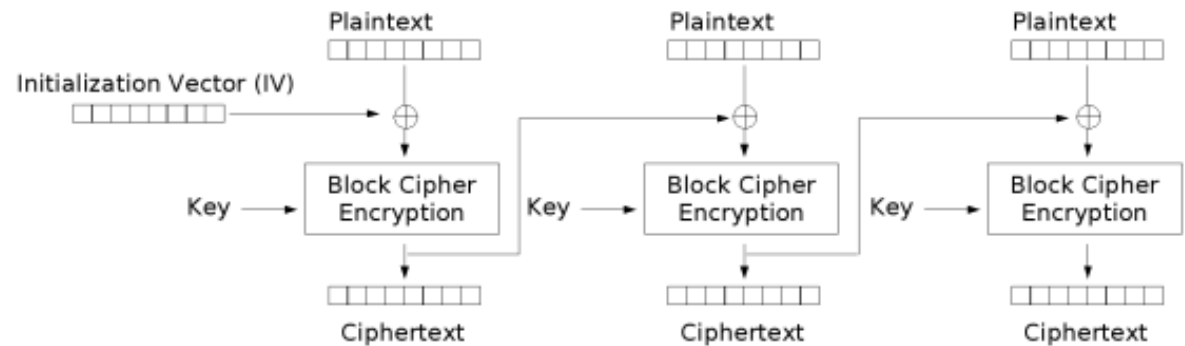


Self-Healing Property

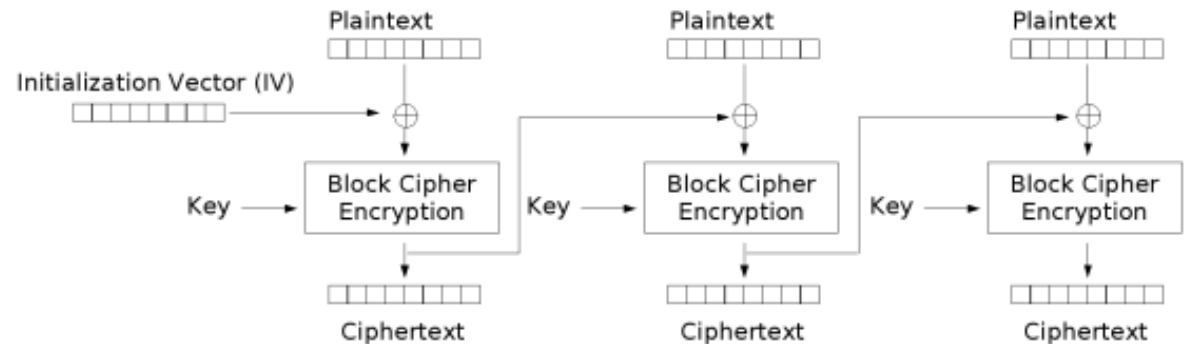
- Initial message
 - 3231343336353837 3231343336353837
3231343336353837 3231343336353837
- Received as (underlined 4c should be 4b)
 - ef7c4cb2b4ce6f3b f6266e3a97af0e2c
746ab9a6308f4256 33e60b451b09603d
- Which decrypts to
 - efca61e19f4836f1 3231333336353837
3231343336353837 3231343336353837
 - Incorrect bytes underlined
 - Plaintext “heals” after 2 blocks

Cipher Block Chaining (CBC) Mode

- Sender varies IV to ensure identical messages encrypt differently
- IV public (for every block except perhaps the first)



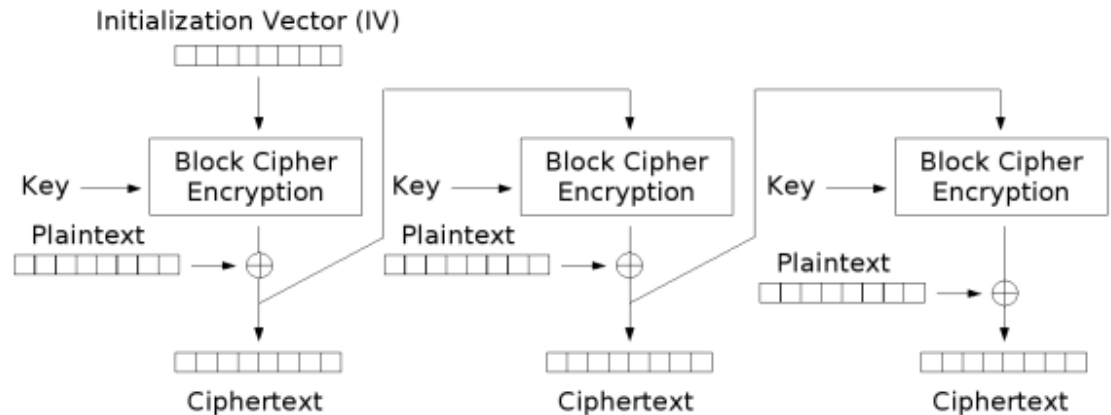
Cipher Block Chaining (CBC) mode encryption



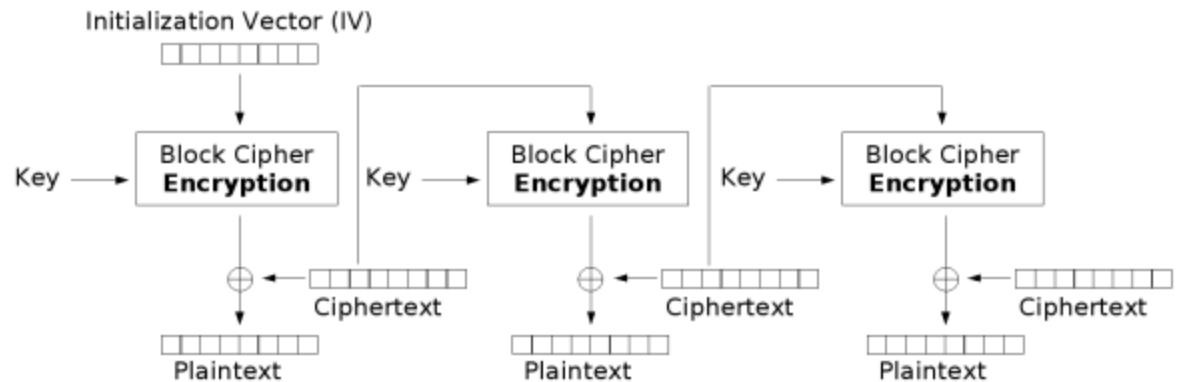
Cipher Block Chaining (CBC) mode encryption

Cipher Feedback (CFB) Mode

- Effect on plaintext is less apparent than CBC.



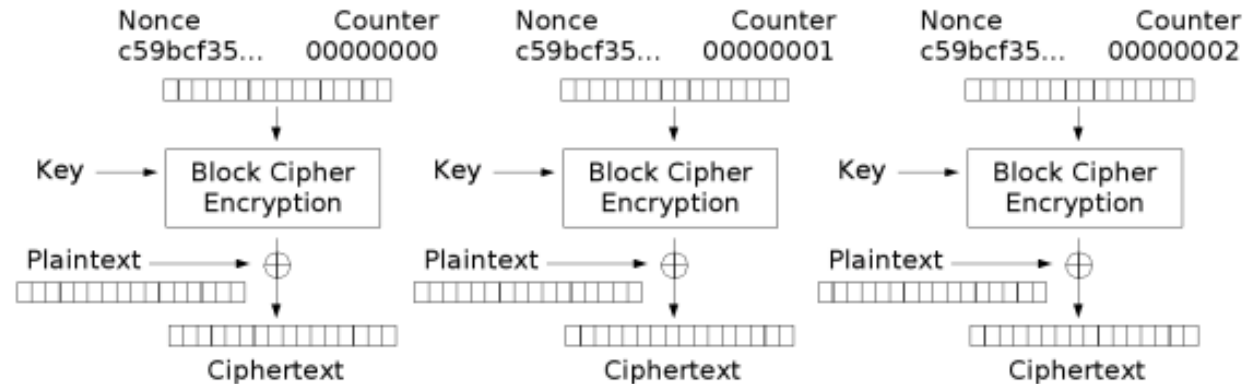
Cipher Feedback (CFB) mode encryption



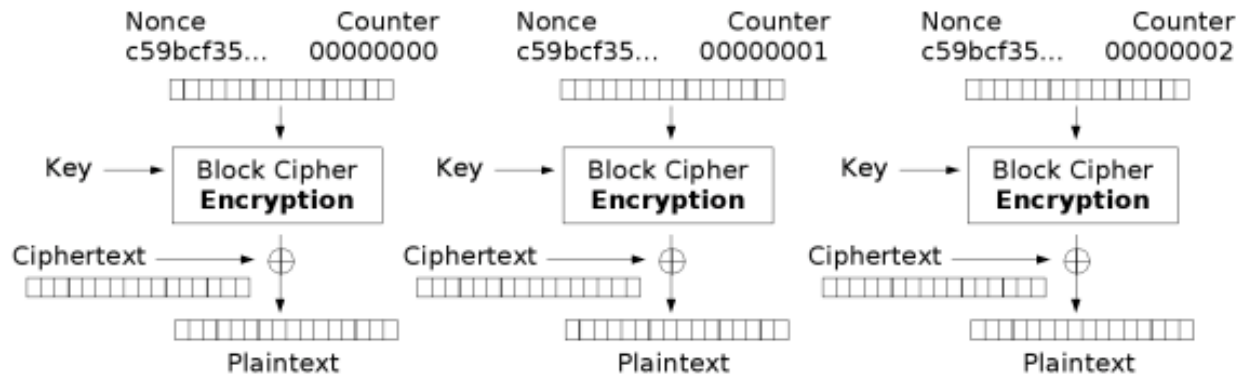
Cipher Feedback (CFB) mode decryption

Counter (CTR) Mode

- Unlike other modes, suitable for *random access* to messages (e.g. encrypting filesystem)



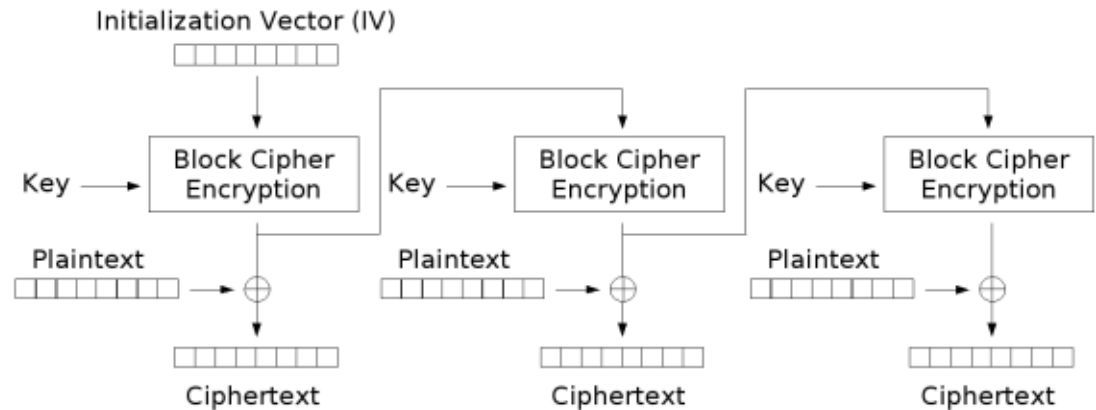
Counter (CTR) mode encryption



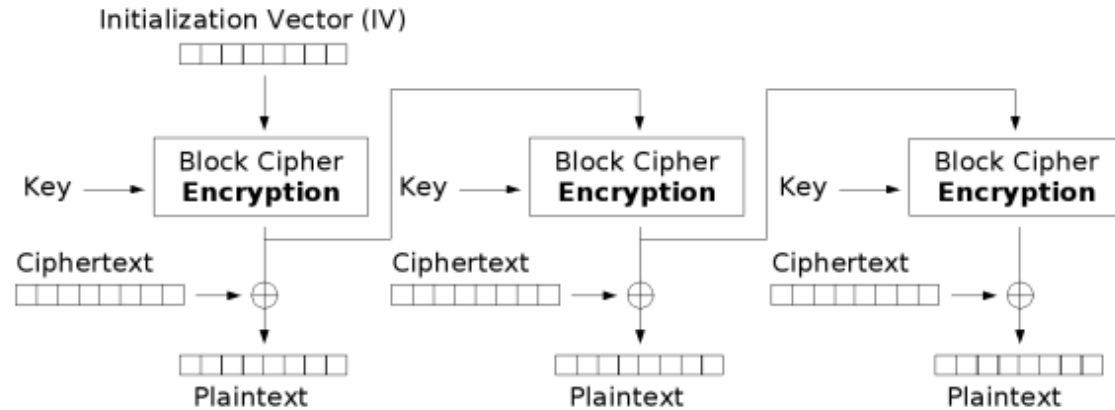
Counter (CTR) mode decryption

Output Feedback (OFB) Mode

- IV and key produce a long stream of bits that can be XORed with plaintext.
- Stream can be used in amounts less than one block size.



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

Stream Ciphers

- Stream cipher: XORs plaintext with a long random or pseudorandom bit string.
- One-Time Pad (OTP): The key is the bit stream and is as long as the message.
- Typically: Use a keyed strong pseudorandom number generator.
- Danger: If two messages are encrypted with the same stream cipher, then the multiple uses of the same bit stream can cancel out:
 - If you know $P \text{ XOR } S$ and $Q \text{ XOR } S$, then you know $P \text{ XOR } Q$.
 - If you know P then you know Q .

What is “strength”?

- How much time (encryptions/decryptions) and how much space (memory) does a search take?
- There are space-time tradeoffs.
- There are shortcuts (e.g. meet-in-the-middle attack).
- Results:
 - DES Double-encryption with two keys requires only twice the time (2^{57} encryptions) (adds one key-bit of strength), if you can store one whole code-book (2^{56} stored blocks)
 - DES Triple-encryption only doubles the effective keylength (to 112 bits).

Current Status of DES

- Design for computer system, associated software that could break any DES-enciphered message in a few days published in 1998
- Several challenges to break DES messages solved using distributed computing
- NIST selected Rijndael as Advanced Encryption Standard, successor to DES
 - Designed to withstand attacks that were successful on DES

Acknowledgements

- Substantial portions of these slides are ©2002-2004 Matt Bishop and used with permission