Betriebsmodi bei Blockchiffren

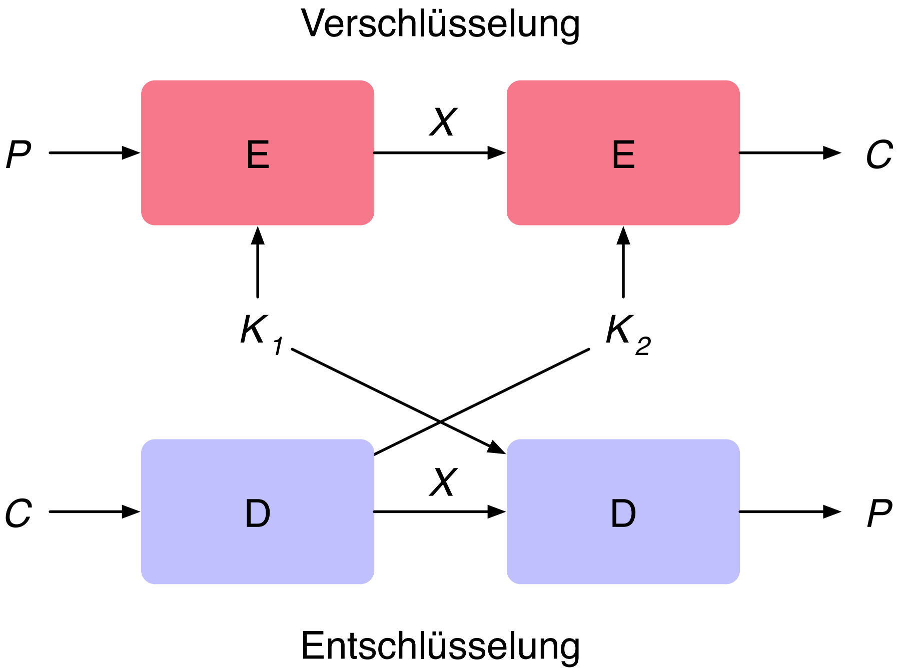
Dozent: Prof. Dr. Michael Eichberg

Version: 2024-02-26

Basierend auf: *Cryptography and Network Security - Principles and Practice, 8th Edition, William Stallings*

DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

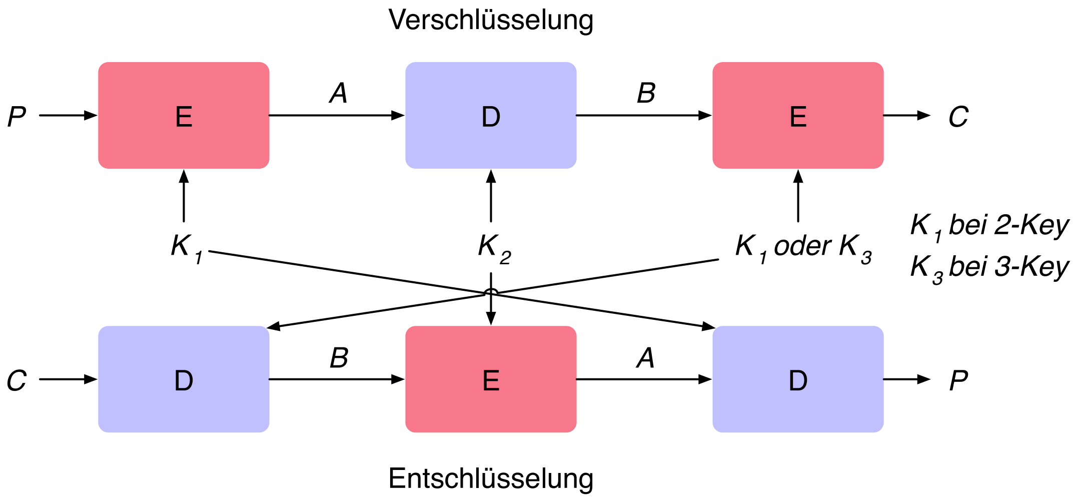
Double Encryption



Meet-in-the-Middle Attack

- Observation: $E(K_2, E(K_1, P)) = E(K_3, P)$ does not hold. I.e., the use of double DES results in a mapping that is not equivalent to a single DES encryption.
- The meet-in-the-middle algorithm will attack this scheme. It does not depend on any particular property of DES but will work against any block encryption cipher.
- The result is that a known plaintext attack against double-DES will succeed with an effort on the order $\mathbf{2}^{56}$ compared to $\mathbf{2}^{55}$ for a single DES.

Triple Encryption (E.g., Triple-DES with Three-Keys)



Triple-DES with Two Keys

Obvious counter to the meet-in-the-middle attack is to use three stages of encryption with three different keys.

- This raises the cost of the meet-in-the-middle attack to 2^{112}, which is beyond what is practical.
- Has the drawback of requiring a key length of $56\,bits \times 3 = 168\,bits$, which may be somewhat unwieldy.
- As an alternative Tuchman proposed a triple encryption method that uses only two keys.
- 3DES with two keys is a relatively popular alternative to DES and has been adopted for use in the key management standards ANSI X9.17 and ISO 8732.

Triple-DES with Three Keys

- Several attacks against 3DES with 2 keys have been developed, which are - however - still not practical.
- Many researchers now feel that three-key 3DES is the preferred alternative.
- Three-key 3DES has an effective key length of 168 bits and is defined as: $C = E(K_3, D(K_2, E(K_1, P)))$
- Backward compatibility with DES is provided by putting: $K_3 = K_2$ or $K_1 = K_2$.

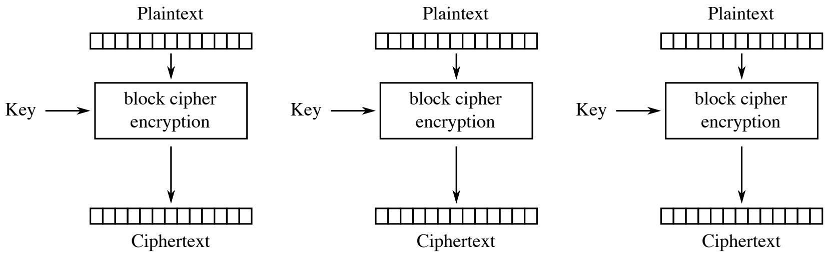
Modes of Operation

- A technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application.
- To apply a block cipher in a variety of applications, five modes of operation have been defined by NIST.
  - The five modes are intended to cover a wide variety of applications of encryption for which a block cipher could be used
  - These modes are intended for use with any symmetric block cipher, including 3DES and AES.

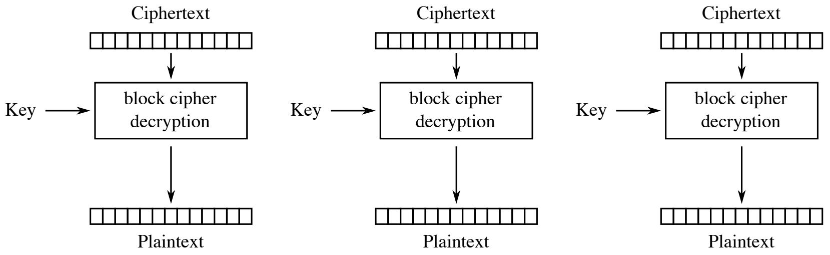
Modes of Operation - Overview

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	▪ Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	▪ General-purpose block-oriented transmission ▪ Authentication
Cipher Feedback (CFB)	Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	▪ General-purpose stream-oriented transmission ▪ Authentication
Output	Similar to CFB, except that the input to the encryption	▪ Stream-oriented transmission over

Electronic Codebook



Electronic Codebook (ECB) mode encryption

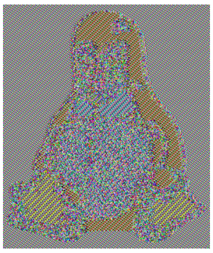


Electronic Codebook (ECB) mode decryption

Author: https://commons.wikimedia.org/wiki/User:WhiteTimberwolf

Problems when using ECB Mode Encryption

ECB-Tux - the linux pinguin encrypted using ECB mode.

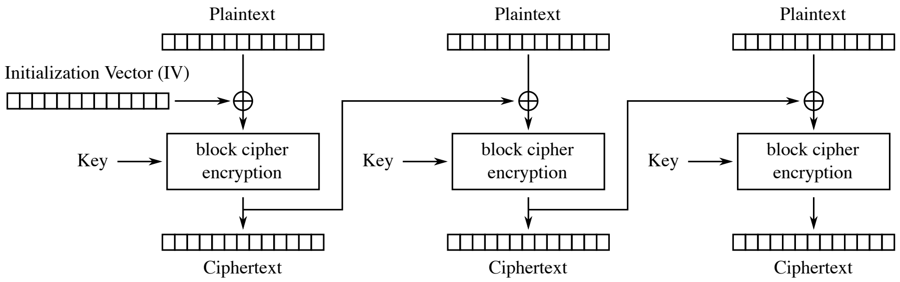


Source: https://github.com/robertdavidgraham/ecb-penguin

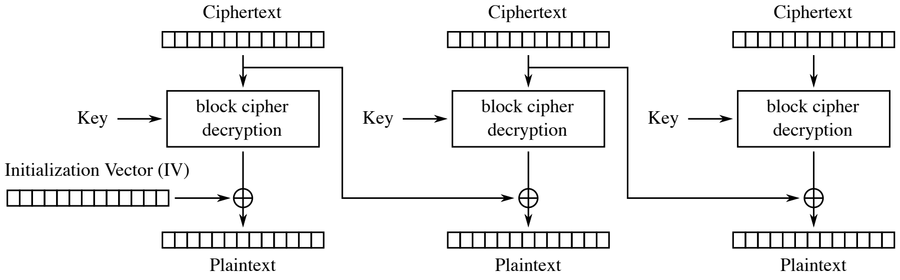
Criteria and properties for evaluating and constructing block cipher modes of operation that are superior to ECB.

- Overhead
- Error recovery
- Error propagation
- Diffusion
- Security

Cipher Block Chaining



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Author: https://commons.wikimedia.org/wiki/User:WhiteTimberwolf

Converting Block Ciphers into Stream Ciphers

For AES, DES, or any block cipher, encryption is performed on a block of b bits:

- In the case of (3)DES $b = 64$
- In the case of AES $b = 128$

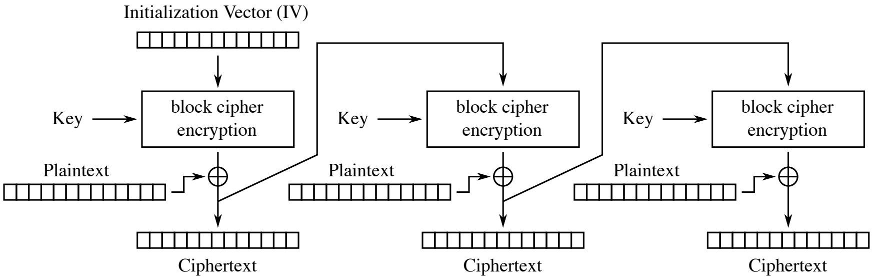
Note

There are three modes that make it possible to convert a block cipher into a character-oriented stream cipher:

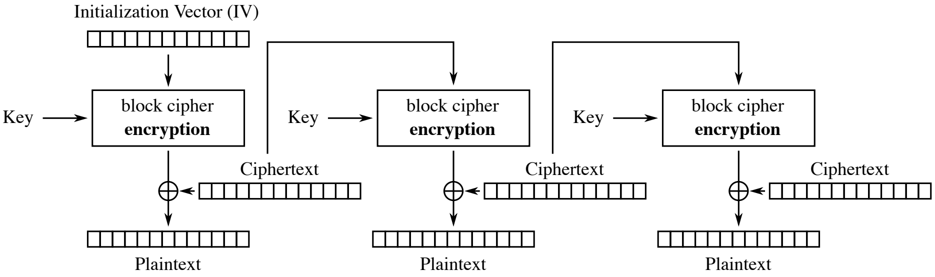
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)
- Counter Mode (CTR)

I.e., no padding is required when the message is not a multiple of the block size.

Cipher Feedback Mode



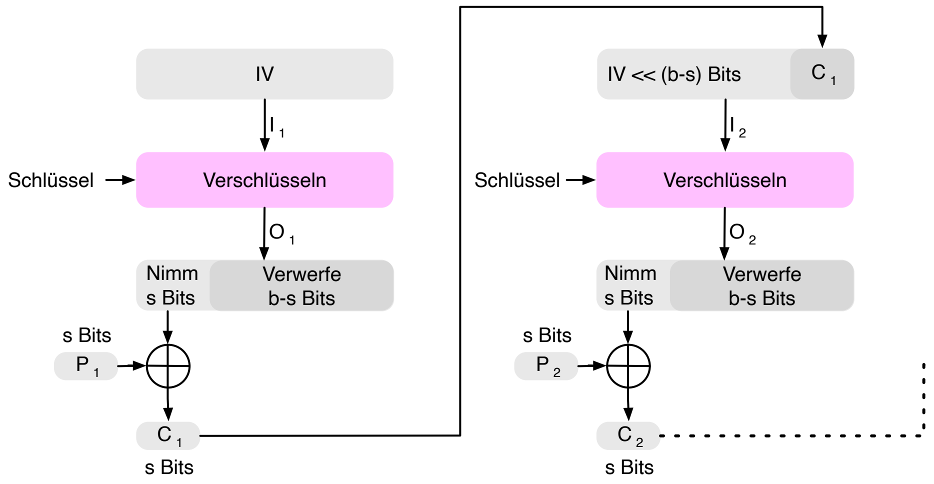
Cipher Feedback (CFB) mode encryption


Initialization Vector (IV)
Key
block cipher **encryption**
Ciphertext
Plaintext
Key
block cipher **encryption**
Ciphertext
Plaintext
Key
block cipher **encryption**
Ciphertext
Plaintext

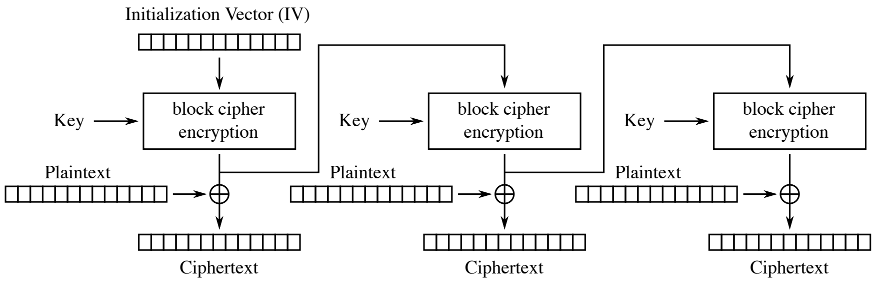
Cipher Feedback (CFB) mode decryption

Author: https://commons.wikimedia.org/wiki/User:WhiteTimberwolf

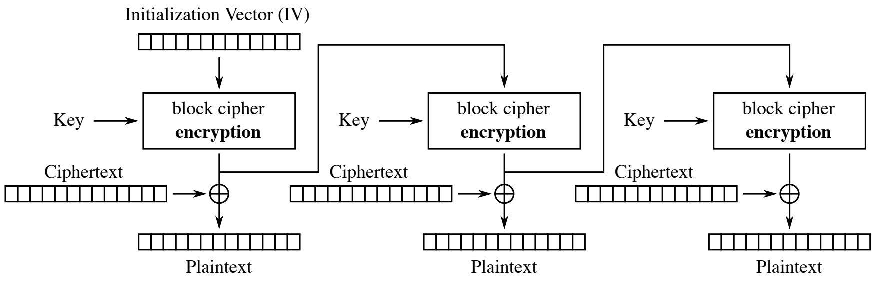
Cipher Feedback Mode used as a Stream Cipher



Output Feedback Mode



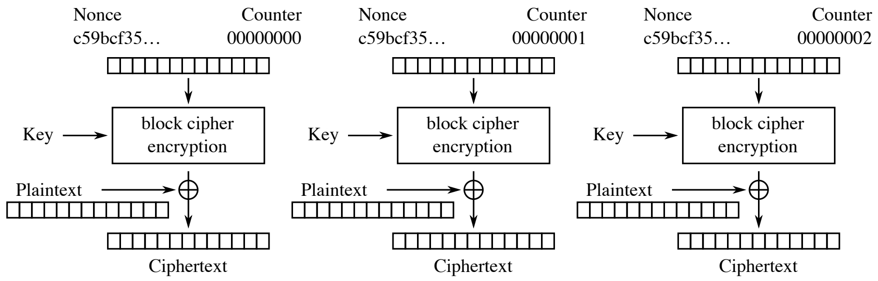
Output Feedback (OFB) mode encryption


Initialization Vector (IV)
Key
block cipher **encryption**
Ciphertext
Plaintext
Key
block cipher **encryption**
Ciphertext
Plaintext
Key
block cipher **encryption**
Ciphertext
Plaintext

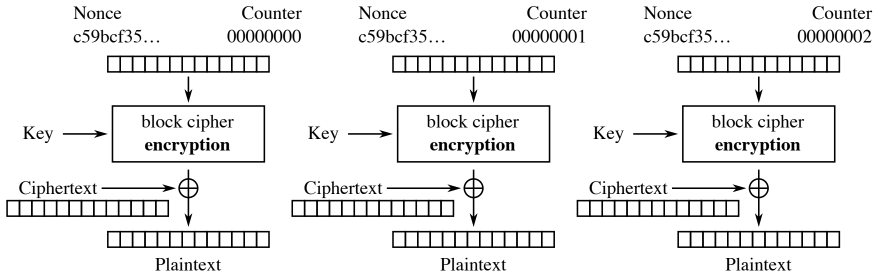
Output Feedback (OFB) mode decryption

Author: https://commons.wikimedia.org/wiki/User:WhiteTimberwolf

Counter Mode



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Author: https://commons.wikimedia.org/wiki/User:WhiteTimberwolf

Counter Mode - Advantages

Hardware efficiency:
can make use of hardware parallelization.

Software efficiency:
easily parallelizable in software.

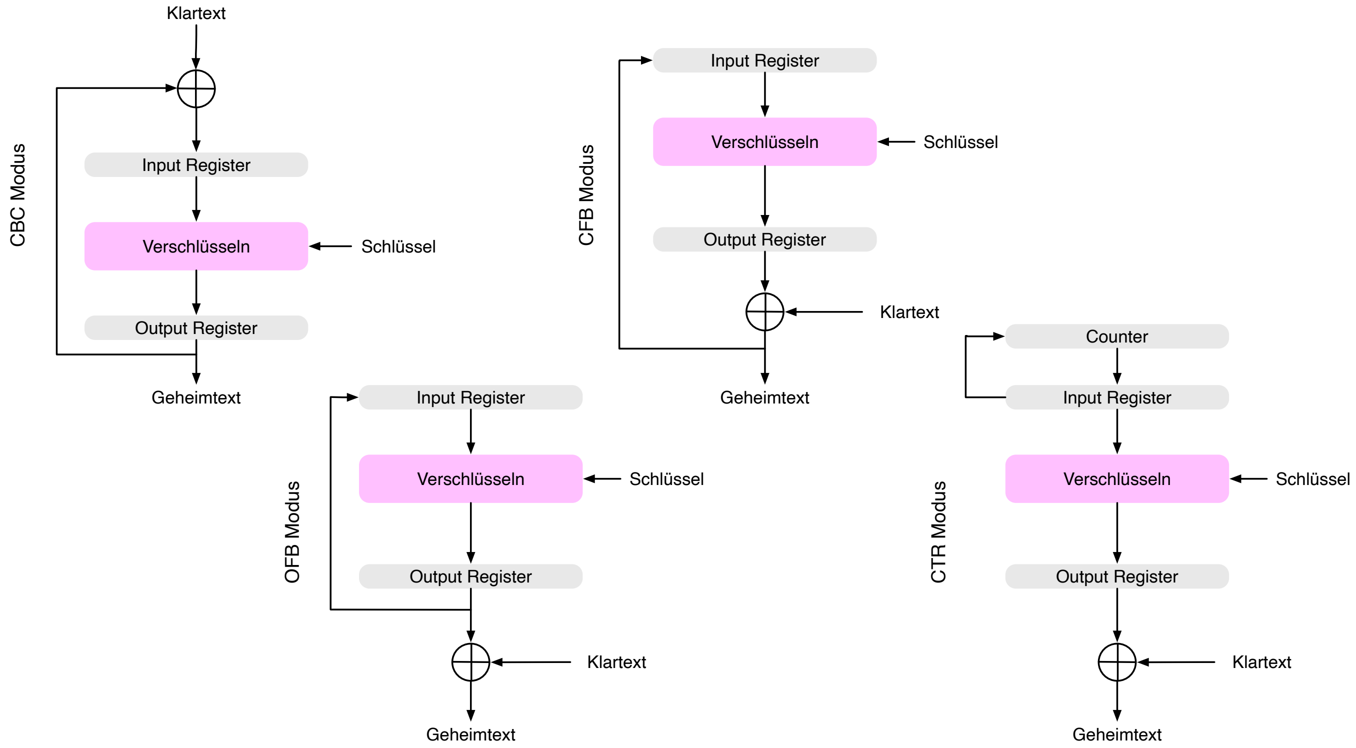
Preprocessing: the encryption of the counters

Random access: The i-th block of plaintext of ciphertext can be processed in random-access fashion.

Provable security: as secure as the other modes

Simplicity: only the encryption algorithm is required.

Feedback Characteristics of Modes of Operation



XTS-AES Mode for Block-Oriented Storage Devices

Approved as an additional block cipher mode of operation by NIST in 2010 Mode is also an IEEE Standard, IEEE Std 1619-2007

- Standard describes a method of encryption for data stored in sector- based devices where the threat model includes possible access to stored data by the adversary.
- Has received widespread industry support

Note

Which potential threats are relevant?

Tweakable Block Ciphers

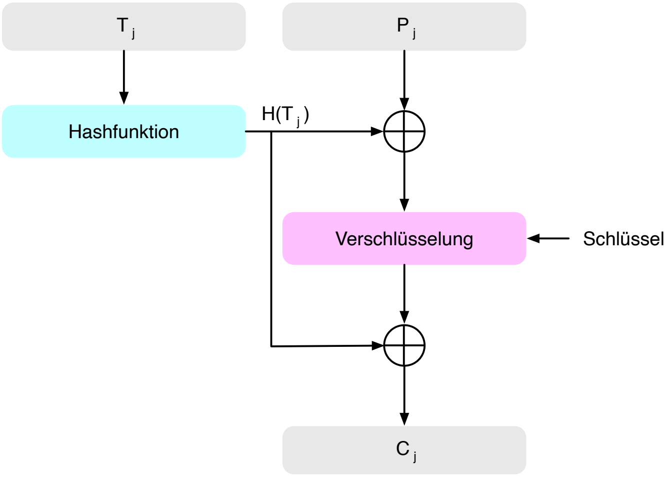
- XTS-AES mode is based on the concept of a tweakable block cipher
- General structure:

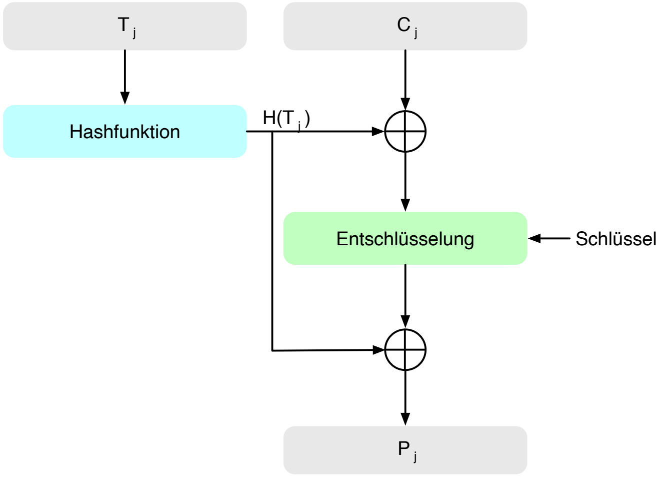
  To compute the ciphertext a:

  - **Plaintext**
  - **Symmetric key**
  - **Tweak**

  is required.
- Tweak need not be kept secret; purpose is to provide variability.

Tweakable Block Ciphers





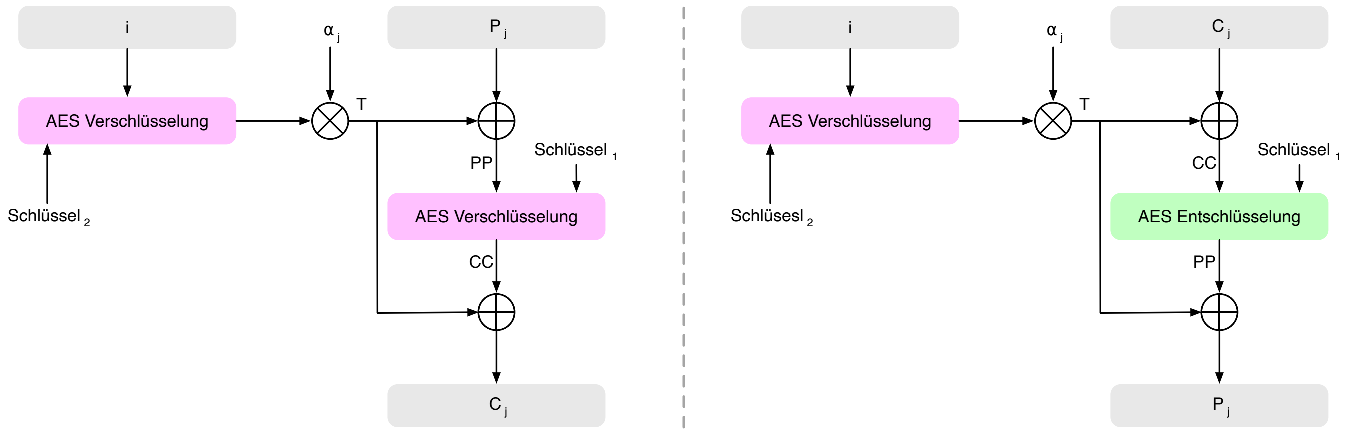
Storage Encryption Requirements

The requirements for encrypting stored data, also referred to as “data at rest”, differ somewhat from those for transmitted data.

The P1619 standard was designed to have the following characteristics:

- The ciphertext is freely available for an attacker.
- The data layout is not changed on the storage medium and in transit.
- Data are accessed in fixed sized blocks, independently from each other.
- Encryption is performed in 16-byte blocks, independently from each other.
- There are no other metadata used, except the location of the data blocks within the whole data set.
- The same plaintext is encrypted to different ciphertexts at different locations, but always to the same ciphertext when written to the same location again.
- A standard conformant device can be constructed for decryption of data encrypted by another standard conformant device.

XTS-AES Operation on a Single Block



Übung

1. Why is it important in CBC to protect the IV?

Solution

If the IV is sent as is, we may be able in certain scenarios to flip some bytes of the plaintext (of the first block) when we change the IV.

2. In which operation modes is padding necessary?

Solution

ECB and CBC (the input to the encryption is a full plaintext block).

3. What happens in case of a transmission error (single bit flip in the ciphertext) in