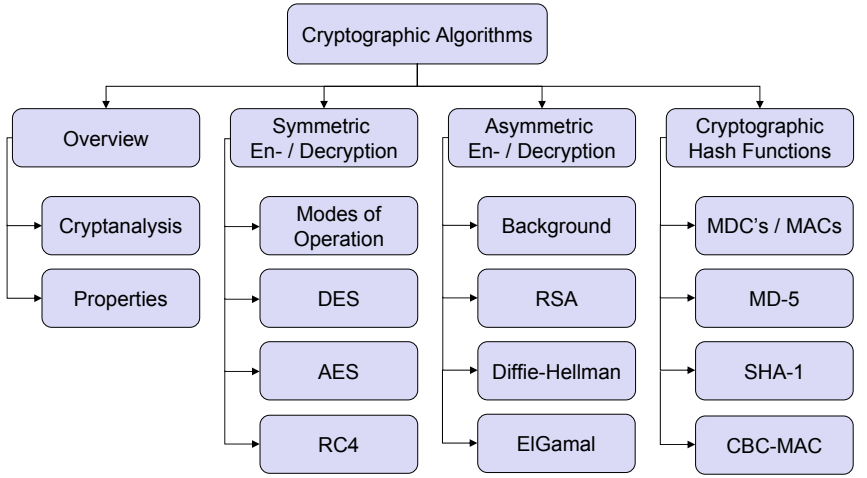
Chair for Network Architectures and Services
Department of Informatics
TU München – Prof. Carle

Network Security

Chapter 2 Basics
2.1 Symmetric Cryptography

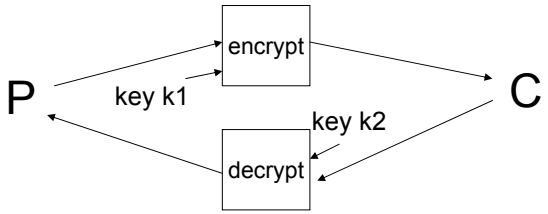
- Overview of Cryptographic Algorithms
- Attacking Cryptographic Algorithms
- Historical Approaches
- Foundations of Modern Cryptography
- Modes of Encryption
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

Cryptographic algorithms: outline



Basic Terms: Plaintext and Ciphertext

- Plaintext P
  - The original readable content of a message (or data).
  - P_netsec = „This is network security“
- Ciphertext C
  - The encrypted version of the plaintext.
  - C_netsec = „Ff iThtIiDjlyHLPRFxvowf“



- In case of symmetric cryptography, k1 = k2.

Basic Terms: Block cipher and Stream cipher

- Block cipher
  - A cipher that encrypts / decrypts inputs of length n to outputs of length n given the corresponding key k.
    - n is block length
  - Most modern symmetric ciphers are block ciphers, e.g. AES, DES, Twofish, …
- Stream cipher
  - A symmetric cipher that generats a random bitstream, called *key stream,* from the symmetric key *k.*
  - Ciphertext = key stream XOR plaintext

Cryptographic algorithms: overview

- During this course two main applications of cryptographic algorithms are of principal interest:
  - *Encryption* of data: transforms plaintext data into ciphertext in order to conceal its meaning
    - Operations: encrypt and decrypt
  - *"Signing"* of data: computes a *check value* or *digital signature* of a given plain- or ciphertext, that can be verified by some or all entities who are able to access the signed data
    - Operations: sign and verify
    - Note: Signing is not always meant in the meaning of a digital signature, but as a method to protect integrity by adding some information that intended recipients can use to check the validity of the message.
- Principal categories of cryptographic algorithms:
  - *Symmetric cryptography* using 1 key for en-/decryption
  - *Asymmetric cryptography* using 2 different keys for en-/decryption
  - *Cryptographic hash functions* using 0 keys (if a symmetric key is used, it is not a separate input but "appended" to or "mixed" with the data).

Attacking cryptography (1): brute force attack

- The *brute force attack* tries every possible key until it finds an intelligible plaintext:
  - Brute Force attacks need that a plaintext is known. Then almost any cipher can be attacked. On average, half of all possible keys will have to be tried.

Average Time Required for Exhaustive Key Search

Key Size [bit]	Number of keys	Time required at 1 encryption / μs	Time required at 10^6 encryption/μs
32	$2^{32} = 4.3 * 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 * 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 * 10^{38}$	2^{127} μs = $5.4 * 10^{24}$ years	$5.4 * 10^{18}$ years

  - 1 encryption / μs: 100 Clock cycles of a 100 MHz processor
  - 10^6 encryptions / μs: Clock cycles using 500 parallel 2GHz processors

Attacking cryptography (2): How large is large?

Reference Numbers Comparing Relative Magnitudes

Reference	Magnitude
Seconds in a year	$\approx 3 * 10^7$
Seconds since creation of solar system	$\approx 2 * 10^{17}$
Clock cycles per year (3 GHz computer)	$\approx 1 * 10^{17}$
Binary strings of length 64	$2^{64} \approx 1.8 * 10^{19}$
Binary strings of length 128	$2^{128} \approx 3.4 * 10^{38}$
Binary strings of length 256	$2^{256} \approx 1.2 * 10^{77}$
Number of 75-digit prime numbers	$\approx 5.2 * 10^{72}$
Electrons in the universe	$\approx 8.37 * 10^{77}$

Attacking cryptography (3): Cryptanalysis

- *Cryptanalysis* is the process of attempting to discover the plaintext and / or the key
- Types of cryptanalysis:
  - *Ciphertext only:* work on ciphertext only; hope that specific patterns of the plaintext have remained in the ciphertext (frequencies of letters, digraphs, etc.)
  - *Known ciphertext / plaintext pairs*
  - *Chosen plaintext or chosen ciphertext*
  - *Differential cryptanalysis, linear cryptanalysis*
- Cryptanalysis of public key cryptography:
  - The fact that one key is publicly exposed may be exploited
  - Public key cryptanalysis is more aimed at breaking the cryptosystem itself and is closer to pure mathematical research than to classic cryptanalysis
  - Important directions:
    - Computation of discrete logarithms
    - Factorization of large integers

A perfect symmetric cipher: One-Time-Pad

- Assumption: Alice and Bob share a perfectly random bitstream otp.
  - All bits are independent and all bits are equally likely 0 or 1.
- Encryption:
  - Alice XORs the message m_i with the next bits otp_i of the bitstream otp.
  - c_i = m_i XOR otp_i
- Decryption:
  - Bob XORs the received ciphertext with the same bits of the otp bitstream.
  - c_i XOR otp_i = (m_i XOR otp_i) XOR otp_i = m_i
- Observation
  - Key has same size as message.
- Cryptanalysis for One-Time-Pad
  - Ciphertext only
    - No attack possible as *any possible plaintext can be generated* with the ciphertext.
  - Even pairs of ciphertext and plaintext hardly help to attack other parts of a message as all unknown parts look perfectly random.

Brute Force attacks on weaker ciphers

- Even on weaker ciphers than One-Time-Pad, a bruteforce attack trying all keys may not be successful.
  - Bruteforce attacks need to be able to check if e.g. a key was the right one.
    - If not, the right one cannot be detected.
  - Usually, a key has a fixed length n.
    - Given m as the length of the message, with m > n (usually m >> n), not all possible plaintexts can be generated anymore.
    - The larger m is, the less likely it gets to hit a plaintext (2^m possible texts) that makes sense by decrypting a given ciphertext with an arbitrary key (only 2^k possible decryptions due to only 2^k possible keys).
- Further issues: no perfect randomness, statistics can be utilized,
- So, if algorithm is weak, the attacker might be able to break it.
  - Or at least find the most likely plaintext.

Classification of modern encryption algorithms

- The type of operations used for transforming plaintext to ciphertext:
  - *Substitution*, which maps each element in the plaintext (bit, letter, group of bits or letters) to another element
  - *Transposition,* which re-arranges elements in the plaintext
- The number of keys used:
  - *Symmetric ciphers,* which use the same key for en- / decryption
  - *Asymmetric ciphers,* which use different keys for en- / decryption
- The way in which the plaintext is processed:
  - *Stream ciphers* work on bit streams and encrypt one bit after another
  - *Block ciphers* work on blocks of width *b* with *b* depending on the specific algorithm.

Basic cryptographic Principles

- Substitution
  - Individual characters are exchanged by other characters

  Types of substitution
  - simple substitution: operates on single letters
  - polygraphic substitution: operates on larger groups of letters
  - monoalphabetic substitution: uses fixed substitution over the entire message
  - polyalphabetic substitution: uses different substitutions at different sections of a message
- Transposition
  - The position of individual characters changes (Permutation)

Transposition: scytale

- Known as early as 7th century BC
- Principle:
  - Wrap parchment strip over a wooden rod of a fixed diameter and write letters along the rod.
  - Unwrap a strip and “transmit”
  - To decrypt, wrap a received over a wooden rod of the same diameter and read off the text.

  → Key is the diameter of the rod

- Example:

```
troops
headii
nthewe
stneed
moresu
pplies
```

⇨ `thnsm predd opoah nrlod eeeis iedus`

- Weakness:
  - Easy to break by finding a suitable matrix transposition.

Monoalphabetic substitution: Atbash

Jeremiah 25:25

And all the kings of the north, far and near, one with another, and all the kingdoms of the world, which are upon the face of the earth: and the king of Sheshach shall drink after them.

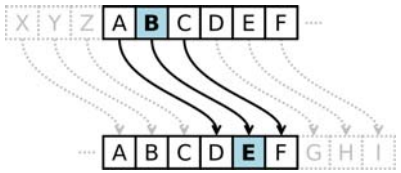
Atbash code: reversed Hebrew alphabet.

A	B	G	D	H	WVFY	Z	H	T	IJ	K	L	M	N	X	O	P	Z	Q	R	S	T
Aleph	Beth	Gimel	Daleth	He	Waw	Zajin	Chet	Tet	Jod	Kaph	Lamed	Mem	Nun	Samech	Ajin	Pe	Sade	Koph	Resch	Sin	Taw
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ ך	ל	מ ם	נ ן	ס	ע	פ ף	צ ץ	ק	ר	ש	ת
T	S	R	Q	Z	P	O	X	N	M	L	K	IJ	T	H	Z	WVFY	H	D	G	B	A
Taw	Sin	Resch	Koph	Sade	Pe	Ajin	Samech	Nun	Mem	Lamed	Kaph	Jod	Tet	Chet	Zajin	Waw	He	Daleth	Gimel	Beth	Aleph
ת	ש	ר	ק	צ ץ	פ ף	ע	ס	נ ן	מ ם	ל	כ ך	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Sheshach ⇨ ש ש ך כ ⇨ ב ב ⇨ ל ל ⇨ Babel

Monoalphabetic substitution: Caesar cipher

- Caesar code: left shift of alphabet by 3 positions.



- Example (letter of Cicero to Caesar):

  `MDEHV RSNQNRQNV PHDH XHVXNPRQNZP`

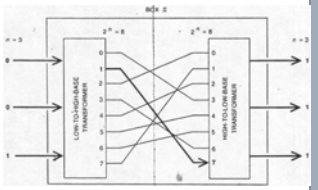
  `HABES OPINIONIS MEAE TESTIMONIUM`

- Weakness: a limited number of possible substitutions. Easy to break by brute force!

Modern cryptography: S and P-boxes

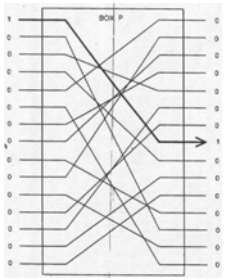
S-box:

- Block-wise **substitution** of binary digits.
  - Can be static or depend on key
  - Input and output size can be different
  - Can be implemented as a large table with all inputs and their predefined outputs
- Resistant to attacks for sufficiently large block size; e.g. for n=128 it provides 2^{128} possible mappings.



P-box:

- Block-wise **permutation** of binary digits.
- Realizes a simple **transposition** cipher with maximal entropy.
- Problem: straightforward attacks exist.

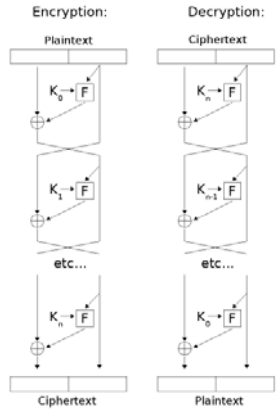


A product cipher of S and P-boxes

- A product cipher is a combination of simple ciphers (e.g. S-box and P-box) to make the cipher more secure.
- Rounds: This combination may be applied multiple times.
- Multiple rounds provide a cryptographically strong polyalphabetic substitution.
- Combination of substitution with transposition provides protection against specific attacks (frequency analysis).
- Follows the theoretical principles outlined by C. Shannon in 1949: combines “confusion” with “diffusion” to attain maximal entropy of a cipher text.
  - *Confusion*: cipher text statistics depend in a very complex way on plaintext statistics (approach: substitution in different rounds)
    - e.g. make the number of 1s and 0s in ciphertext seem independent of their numbers in plaintext
  - *Diffusion*: each digit in plaintext and in key influence many digits of cipher text (approach: many rounds with transposition)

Feistel ciphers (Feistel network)

- A multiple-round scheme with separate keys per round.
- Goal: Encrypt plaintext block $P = L_0 \mid R_0$
- Function $f(K_i, R_{i-1})$ is algorithm-specific, usually a combination of permutations and substitutions.
- Invertible via a reverse order of rounds.
- 3 rounds suffice to achieve a pseudorandom permutation.
- 4 rounds suffice to achieve a strong pseudorandom permutation (i.e. it remains pseudorandom to an attacker with an oracle access to its inverse permutation).
- A foundation for a large number of modern symmetric ciphers: DES, Lucifer, Blowfish, RC5, Twofish, etc.



Feistel Cipher

Symmetric Block Ciphers - Algorithm Overview

- Some popular algorithms:
  - Data Encryption Standard (DES)
  - Triple encryption with DES: Triple-DES
  - Advanced Encryption Standard (AES)
  - Twofish
  - Stream Cipher Algorithm RC4

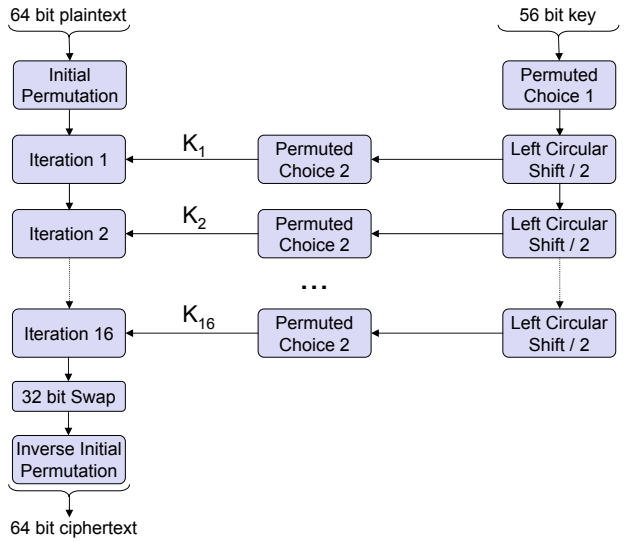
The Data Encryption Standard (DES) – History

- 1973 the National Bureau of Standards (NBS, now National Institute of Standards and Technology, NIST) issued a request for proposals for a national cipher standard, demanding the algorithm to:
  - provide a high level of security,
  - be completely specified and easy to understand,
  - provide security only by its key and not by its own secrecy,
  - be available to all users,
  - be adaptable for use in diverse applications,
  - be economically implementable in electronic devices,
  - be efficient to use,
  - be able to be validated, and
  - be exportable.
- None of the submissions to this first call came close to these criteria.
- In response to a second call, IBM submitted its’ algorithm LUCIFER, a symmetric block cipher, which works on blocks of length 128 bit using keys of length 128 bit and that was the only promising candidate

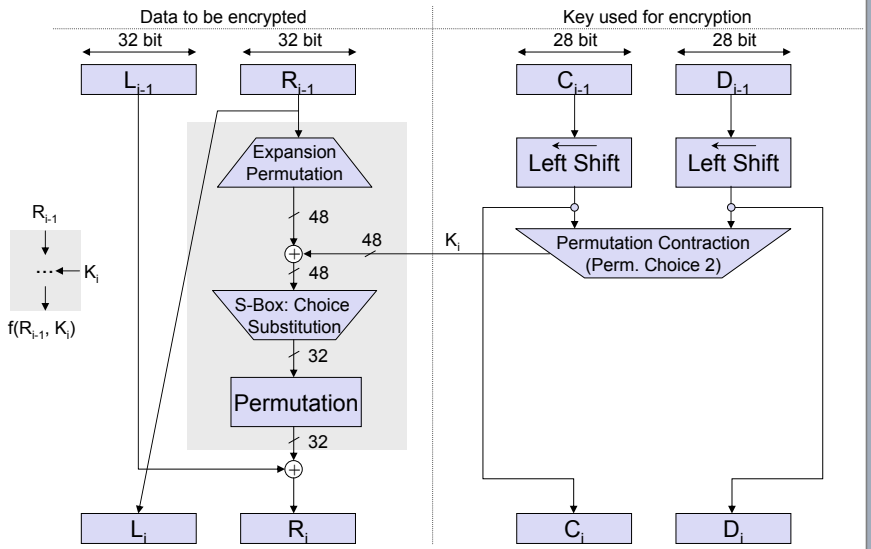
DES – History continued

- The NBS requested the help of the National Security Agency (NSA) in evaluating the algorithm's security:
  - The NSA reduced the block size to 64 bit, the size of the key to 56 bit and changed details in the algorithm's *substitution boxes.*
  - Many of the NSA's reasoning for these modifications became clear in the early 1990s, but raised great concern in the late 1970s.
- Despite all criticism the algorithm was adopted as "Data Encryption Standard" in the series of Federal Information Processing Standards in 1977 (FIPS PUB 46) and authorized for use on all unclassified government communications.
- DES was widely adopted in the years to follow

DES – Algorithm Outline



DES – Single Iteration



DES – Security

- Main weakness is the key length:
  - As a 56 bit key can be searched in 10.01 hours when being able to perform 10^6 encryptions / µs (which is feasible today), DES can no longer be considered as sufficiently secure
- *Differential cryptanalysis:*
  - In 1990 E. Biham and A. Shamir published a cryptoanalysis method for DES
  - It looks specifically for differences in ciphertexts whose plaintexts have particular differences and tries to guess the correct key
  - The basic approach needs **chosen plaintext** together with its **ciphertext**
  - DES with 16 rounds is immune against this attack, as the attack needs 2^{47} chosen plaintexts or (when "converted" to a known plaintext attack) 2^{55} known plaintexts.
  - The designers of DES told in the 1990s that they knew about this kind of attacks in the 1970's and that the S-boxes were designed accordingly

Extending the Key-Length of DES by Multiple Encryption

- Triple encryption scheme, as proposed by W. Tuchman in 1979:
  - $C = E(K_3, D(K_2, E(K_1, P)))$
  - The use of the decryption function *D* in the middle allows to use triple encryption devices with peers that only own single encryption devices by setting $K_1 = K_2 = K_3$ (backwards compatibility with DES)
  - Triple encryption can be used with two (set $K_1 = K_3$) or three different keys
  - There are no known practical attacks against this scheme up to now
  - Drawback: the performance is only 1/3 of that of single encryption, so it should be a better idea to use a different cipher, which offers a bigger key-length right away
- Double encryption is not a feasible option – there is an attack against it (Meet-in-the-middle-attack)

The Advanced Encryption Standard AES (1)

- Jan. 1997: the *National Institute of Standards and Technology (NIST)* of the USA announces *the AES development* effort.
  - The overall goal is to develop a Federal Information Processing Standard (FIPS) that specifies an encryption algorithm(s) capable of protecting sensitive government information well into the next century.
  - The algorithm(s) is expected to be used by the U.S. Government and, on a voluntary basis, by the private sector.
- Sep. 1997: formal *call for algorithms*, open to everyone
  - AES would specify an unclassified, publicly disclosed encryption algorithm(s), available royalty-free, worldwide.
  - The algorithm(s) must implement symmetric key cryptography as a block cipher and (at a minimum) support block sizes of 128-bits and key sizes of 128-, 192-, and 256-bits.
- Aug. 1998: first AES candidate conference
  - NIST announces the selection of 15 candidate algorithms
  - Demand for public comments

The Advanced Encryption Standard AES (2)

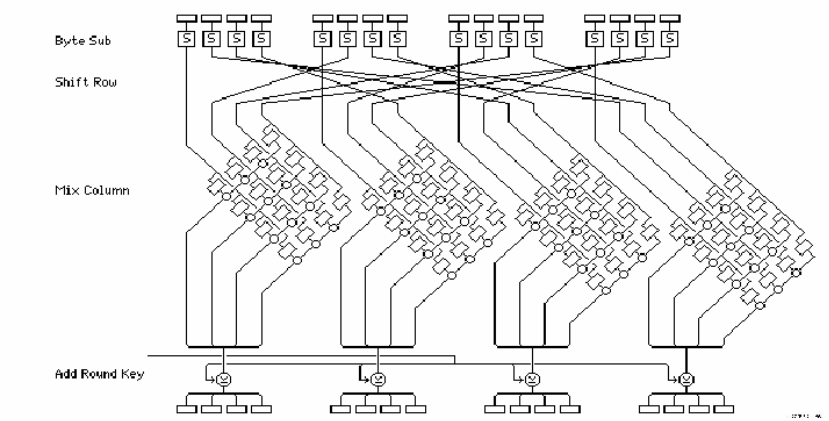
- Mar. 1999: second AES candidate conference
  - Discussion of results of the analysis conducted by the global cryptographic community on the candidate algorithms.
- April 1999:
  - Using the analyses and comments received, NIST selects five algorithms as finalist candidates: *MARS, RC6, Rijndael, Serpent,* and *Twofish*
  - Demand for public comments on any aspect of the finalists:
    - Cryptanalysis
    - Implementation issues
    - Intellectual property & Overall recommendations
- May 2000: third AES candidate conference
- October 2000: Rijndael is announced as NIST's proposal for AES
- 28. February 2001: draft FIPS standard is published [AES01a]
- 29. May 2001: comment period ends
- 26. November 2001: official announcement of the AES standard

The Advanced Encryption Standard AES (3)

- Key and block lengths:
  - Key Length: 128, 192, or 256 bit
  - Block Length: 128, 192, or 256 bit
  - In the following only 128 bit is considered
- Number of rounds: 10 (for block and key size of 128 bit)
  - Rounds 1 - 9 make use of four different operations:
    - ByteSub: a non-linear byte substitution (basically an s-box), specifically designed to work against differential and linear cryptanalysis
    - ShiftRow: the rows of the state are cyclically shifted by various offsets → aims to increase diffusion
    - MixColumn: an operation based on polynomial algebra → aims to increase diffusion
    - RoundKey: a round-key is XORed with the state
  - Round 10 does not make use of the MixColumn operation

The Advanced Encryption Standard AES (4)

Structure of one Round in Rijndael



(source: "Rijndael", a presentation by J. Daemen and V. Rijmen)

Properties of AES

- Roughly 3 times the speed of DES (200 MBit/s vs. 80 MBit/s)
  - Speed was critical in the selection of Rijndael as AES
  - Other ciphers were considered stronger, but slower
  - Rijndael seemed to be the best overall choice
- Can be used in CBC or CTR modes in communication.
- Highly parallel architecture

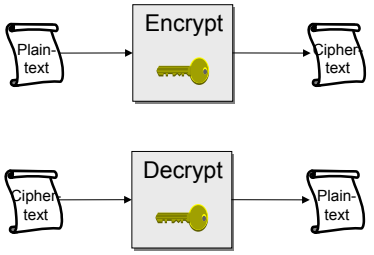
- From the NIST report:
  - "Rijndael appears to offer an adequate security margin. [There is] some criticism on two grounds: that its security margin is on the low side […], and that its mathematical structure may lead to attacks. However, its structure is fairly simple."
  - "Twofish appears to offer a high security margin. […] Twofish has received some criticism for its complexity."

Properties of AES

- Currently still considered secure.
- Until about 2009, AES was considered very secure, but:
  - Its position has been somewhat weakened
    - Description of AES in 8,000 quadratic equations, sparse matrix
      → XSL attack: not workable as such, but has caused some concern
    - Related-key attack on 256 bit AES with 11 rounds
      (full AES has 14 rounds at 256 bit) → does not extend to AES 128 bit, but reduces safety margin
  - A major criticism is that the algebraic description, while elegant, is not well-understood → someone might come up with a linear description
  - Known good attacks are side-channel attacks (timing) – these do not attack the algorithm itself, and are usually impractical
- AES seems to be the best we have, and it is among the most researched algorithms.

Symmetric Encryption (revisited)

- General description:
  - The same key $K_{A,B}$ is used for enciphering and deciphering of messages:



- Notation
  - If P denotes the plaintext message, $E(K_{A,B}, P)$ denotes the cipher text. The following holds: $D(K_{A,B}, E(K_{A,B}, P)) = P$
  - Alternatively we sometimes write $\{P\}_{K_{A,B}}$ or $E_{K_{A,B}}(P)$ for $E(K_{A,B}, P)$
- Symmetric encryption
  - $E_{K_{A,B}}$ is at least an injective, often a bijective function
  - $D_{K_{A,B}}$ is the inverse function of $E_{K_{A,B}}$: $D_{K_{A,B}} = (E_{K_{A,B}})^{-1}$
- Examples: DES, 3DES, AES, Twofish, RC4

Important properties of encryption algorithms

Consider, a sender is encrypting plaintext messages P_1, P_2, ... to ciphertext messages C_1, C_2, ...

Then the following properties of the encryption algorithm, besides its security, are of interest:

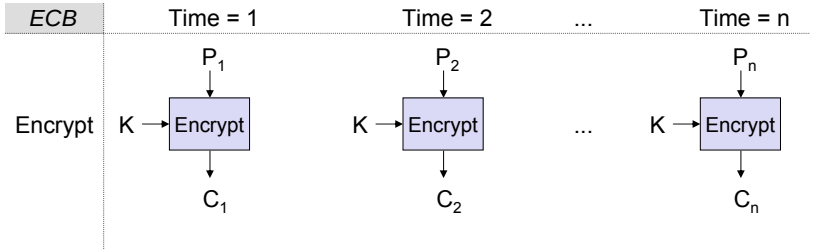
- *Error propagation* characterizes the effects of bit-errors during transmission of ciphertext on reconstructed plaintext P_1', P_2', ...
  - Depending on the encryption algorithm there may be one or more erroneous bits in the reconstructed plaintext per erroneous ciphertext bit
- *Synchronization* characterizes the effects of lost ciphertext data units on the reconstructed plaintext
  - Some encryption algorithms cannot recover from lost ciphertext and need therefore explicit re-synchronization in case of lost messages
  - Other algorithms do automatically re-synchronize after 0 to n (n depending on the algorithm) ciphertext bits

Modes of Encryption

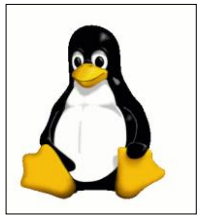
- Block ciphers operate on 128-256 bits. How can one encrypt longer messages? Answer:
  - A plaintext p is segmented in blocks p_1, p_2, ... each of length b or of length $j<b$ when payload length is smaller or not a multiple of b. b denotes the block size of the encryption algorithm.
  - The ciphertext c is the combination of c_1, c_2, ... where c_i denotes the result of the encryption of the i^{th} block of the plaintext message
  - The entities encrypting and decrypting a message have agreed upon a key K.
- Modes where the plaintext is input to the block cipher. Examples:
  - Electronic Code Book Mode (ECB), Cipher Block Chaining Mode (CBC)
- Modes where the plaintext is XORed with the output of a block cipher
  - A pseudorandom stream of bits, called *key stream,* is generated from the symmetric key K and a specific input per block, e.g. E(K,"Block 1"), E(K,"Block 2"), E(K,"Block 3"), …
  - Examples
    - Output Feedback Mode (OFB), Counter Mode (CTR)

Symmetric Block Ciphers - Modes of Encryption – ECB (1)

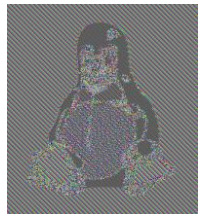
- *Electronic Code Book Mode (ECB):*
  - Every block p_i of length b is encrypted independently: $c_i = E(K, p_i)$
  - A bit error in one ciphertext block c_i results in a completely wrongly recovered plaintext block p_i' (subsequent blocks are not affected)
  - Loss of synchronization does not have any effect if integer multiples of the block size b are lost.
    If any other number of bits are lost, explicit re-synchronization is needed.
  - Drawback: identical plaintext blocks are encrypted to identical ciphertext!



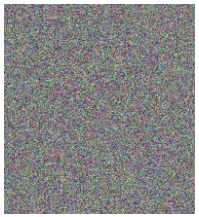
Symmetric Block Ciphers - Modes of Encryption – ECB (2)



Original



Encrypted using ECB mode



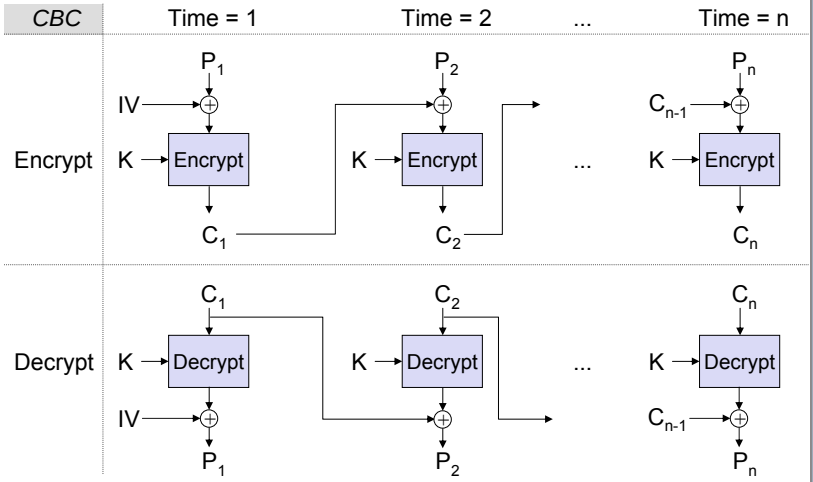
Encrypted using other modes

Source: http://www.wikipedia.org/

Symmetric Block Ciphers - Modes of Encryption – CBC (1)

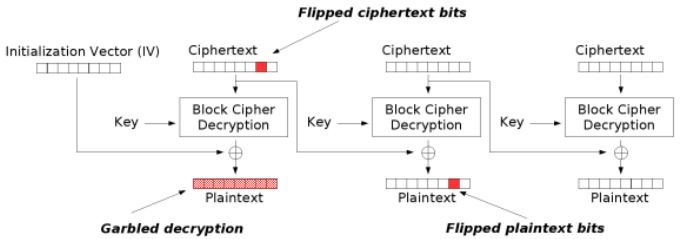
- *Cipher Block Chaining Mode (CBC):*
  - Before encrypting a plaintext block p_i , it is XORed (⊕) with the preceding ciphertext block c_{i-1}:
    - $c_i = E(K, c_{i-1} \oplus p_i)$
    - $p_i' = c_{i-1} \oplus D(K, c_i)$
  - Both parties agree on an *initial value* for c_i *called Initialization Vector (IV)*
    - c_0 = IV
- Properties:
  - Advantage: identical plaintext blocks are encrypted to non-identical ciphertext.
  - Error propagation:
    - A distorted ciphertext block results in two distorted plaintext blocks, as p_i' is computed using c_{i-1} and c_i
  - Synchronisation:
    - If the number of lost bits is a multiple integer of *b,* one additional block p_{i+1} is misrepresented before synchronization is re-established.
      If any other number of bits are lost explicit re-synchronization is needed.
  - Applicable for
    - Encryption
    - Integrity check: use last block of CBC as Message Authentication Code (MAC)

Symmetric Block Ciphers - Modes of Encryption – CBC (2)



CBC Error Propagation

- A distorted ciphertext block results in two distorted plaintext blocks, as p_i' is computed using c_{i-1} and c_i



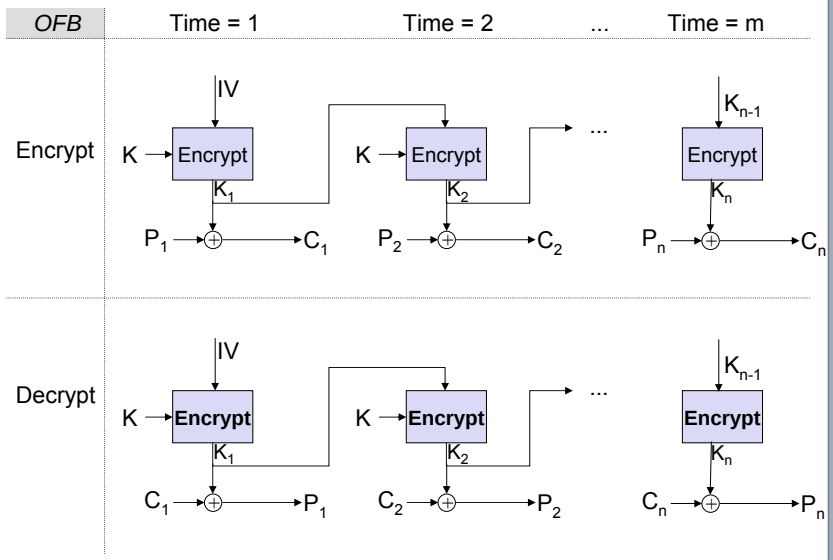
Modification attack or transmission error for CBC

Source: http://www.wikipedia.org/

Symmetric Block Ciphers - Modes of Encryption – OFB (1)

- *Output Feedback Mode (OFB):*
  - The block encryption algorithm is used to generate a key stream that depends only on *K* and *IV*
    - $K_0 = IV$
    - $K_i = E(K,K_{i-1})$
    - $C_i = P_i \oplus K_i$
  - The plaintext blocks are XORed with the pseudo-random sequence to obtain the ciphertext and vice versa

Symmetric Block Ciphers - Modes of Encryption – OFB (2)



Symmetric Block Ciphers - Modes of Encryption – OFB (3)

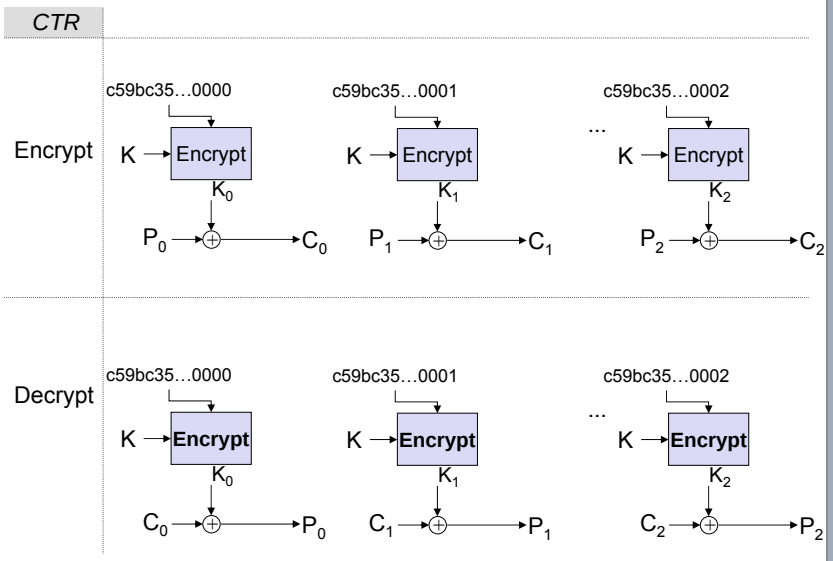
- Properties of OFB:
  - Error propagation:
    - Single bit errors result only in single bit errors ⇒ no error multiplication
  - Synchronisation:
    - If some bits are lost explicit re-synchronization is needed
  - Advantage:
    - The pseudo-random sequence can be pre-computed in order to keep the impact of encryption to the end-to-end delay low
  - Drawbacks:
    - It is possible for an attacker to manipulate specific bits of the plaintext

    → However, additional cryptographic means are can be used for message integrity

Symmetric Block Ciphers – Modes of Encryption - CTR (1)

- *Counter Mode (CTR)*
  - The block encryption algorithm is used to generate a key stream that depends on *K* and a counter function ctr_i .
  - The counter function can be simply an increment modulo 2^w, where *w* is a convenient register width, e.g.
    - $ctr_i = Nonce \,||\, i$
  - The counter function does not provide any security other than the uniqueness of the input to the block cipher function *E*
  - The plaintext blocks are XORed with the pseudo-random sequence to obtain the ciphertext and vice versa
  - Putting everything together:
    - $K_i = E(K, Nonce \,||\, i)$
    - $C_i = P_i \oplus K_i$

Symmetric Block Ciphers – Modes of Encryption - CTR (2)



Symmetric Block Ciphers – Modes of Encryption - CTR (3)

- Properties of CTR:
  - Error propagation:
    - Single bit errors result only in single bit errors ⇒ no error multiplication
  - Synchronisation:
    - If some bits are lost explicit re-synchronization is needed.
  - Advantage:
    - The key stream can be pre-computed in order to keep the impact of encryption to the end-to-end delay low.
    - The computation of the key stream can be parallelized.
  - Drawbacks:
    - It is possible for an attacker to manipulate specific bits of the plaintext

    → However, additional cryptographic means are required for message integrity

Additional References

[AES01a] National Institute of Standards and Technology (NIST). *Specification for the Advanced Encryption Standard (AES).* Federal Information Processing Standards Publication, February 2001.

[DR97a] J. Daemen, V. Rijmen. *AES Proposal: Rijndael.* http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1997.

[FMS01a] S. Fluhrer, I. Mantin, A. Shamir. *Weaknesses in the Key Scheduling Algorithm of RC4.* Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[Riv01a] R. Rivest. *RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4*. http://www.rsa.com/rsalabs/technotes/wep.html, 2001.

[SIR01a] A. Stubblefield, J. Ioannidis, A. D. Rubin. *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP.* AT&T Labs Technical Report TD-4ZCPZZ, August 2001.