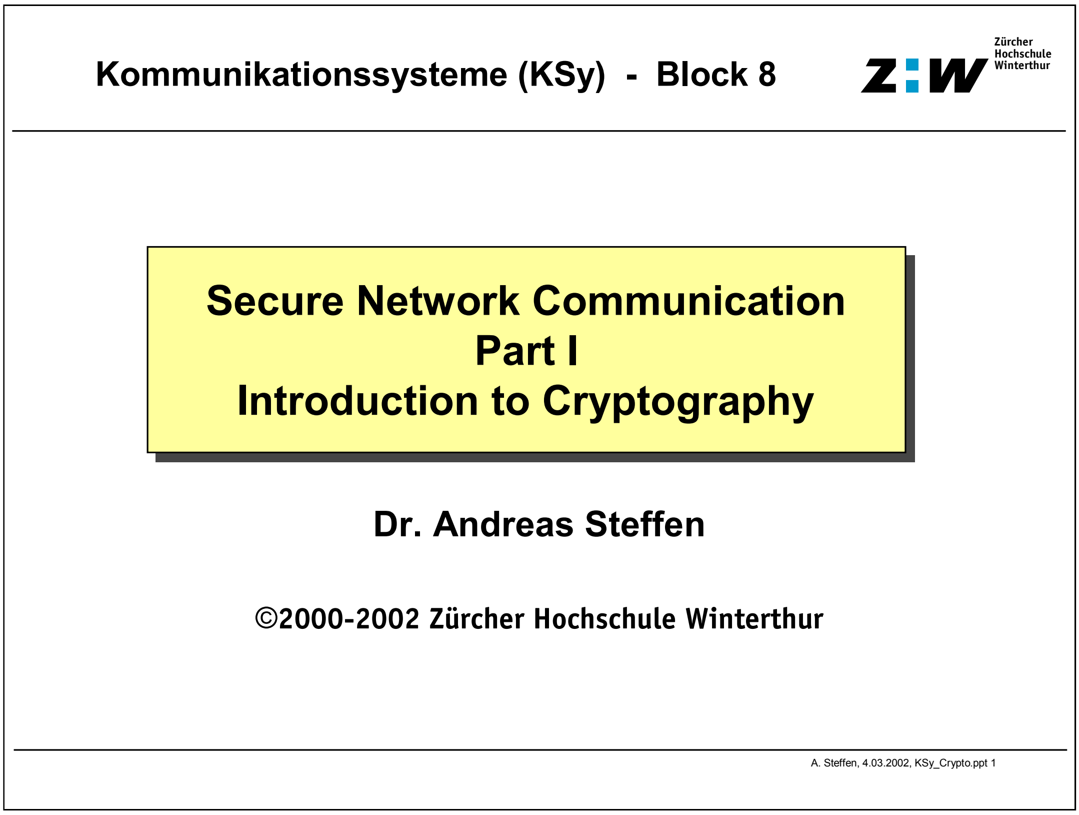


Kommunikationssysteme (KSy) - Block 8

Zürcher Hochschule Winterthur

Secure Network Communication
Part I
Introduction to Cryptography

Dr. Andreas Steffen

A. Steffen, 4.03.2002, KSy_Crypto.ppt 1

Introduction

- Recommended literature
- Terminology

Cryptanalysis

- Fundamental assumptions
- Types of attacks
- Redundancy of natural language texts

Claude Shannon

- Principle of confusion - substitution
- Principle of diffusion - transposition and permutation
- Entropy of English texts
- Perfect secrecy – the one-time pad
- General model of a secrecy system

Symmetric Key Cryptosystems – Block Ciphers

- Common block and key sizes
- Electronic code book mode (ECB)
- Cipher block chaining mode (CBC)

Block Ciphers – Present and Future Standards

- Some popular block ciphers (DES, 3DES, IDEA, CAST, Blowfish, RC2, RC5)
- Digital Encryption Standard (DES) – rounds of confusion and diffusion
- Feistel networks
- Advanced Encryption Standard (AES)
- AES finalists (MARS, RC6, Twofish, Serpent, Rijndael)

Symmetric Key Cryptosystems – Stream Ciphers

- Linear feedback shift registers (LFSRs)
- RC4
- Output feedback mode (OFB) – block ciphers used as stream ciphers

Overview

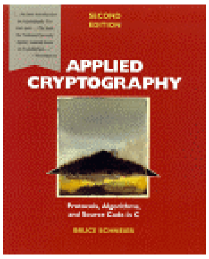
- Week 1 - Introduction to Cryptography
  - Definitions and Basic Principles
  - Cryptanalysis based on Plaintext Redundancy
  - Symmetric Key Cryptosystems
    - Block Ciphers (DES, 3DES, AES)
    - Stream Ciphers (Linear Feedback Shift Registers, RC4)
- Week 2 - Public Key Cryptosystems
  - Finite Field Algebra
    - Addition and Multiplication, Inverses, Fast Exponentiation
  - Public Key Cryptosystems
    - Diffie-Hellmann Key Exchange
    - RSA Public Key Cryptosystem
- Week 3 - Secure Network Applications
  - Secure e-mail (S/MIME, PGP)
  - Secure Socket Layer (SSL)

Cryptography - Literature

Modern Cryptography

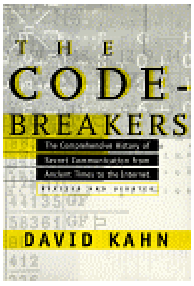
- Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition", 784 pages, 1996, John Wiley & Sons, ISBN 0-471-11709-9

  http://www.counterpane.com



History of Cryptography

- David Kahn, "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet", 1181 pages, 1996, Scribner Book Company, ISBN 0-684-83130-9


THE CODE-BREAKERS
The Comprehensive History of Secret Communication from Ancient Times to the Internet
DAVID KAHN

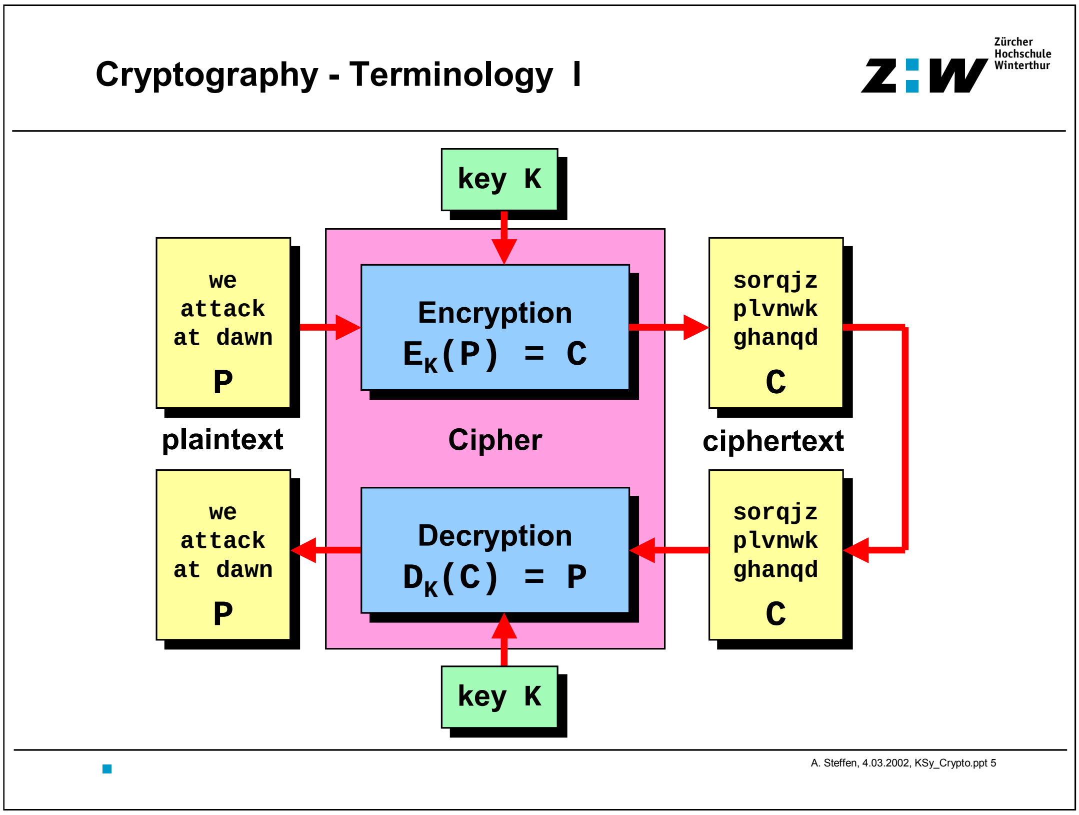
Cryptography - Literature (light)

- Studienarbeit „Kryptographische Verfahren“
  - Jörn Jachalsky, "Untersuchung kryptographischer Verfahren in der TCP/IP-Protokollarchitektur", 131 pages, 1997, Universität Hannnover, Lehrgebiet Rechnernetze und Verteilte Systeme

    http://www.rvs.uni-hannover.de/arbeiten/studien/sa-jacha.html

- The Code Book
  - Simon Singh, "The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography", 410 pages, 2000,

    Anchor Books/Doubleday, ISBN 0-385-49532-3
    Fourth Estate, ISBN 1-857-02889-9



Cryptography - Terminology I

Zürcher Hochschule Winterthur

key K

we attack at dawn

P

Encryption

$E_K(P) = C$

sorqjz plvnwk ghanqd

C

plaintext

Cipher

ciphertext

we attack at dawn

P

Decryption

$D_K(C) = P$

sorqjz plvnwk ghanqd

C

key K

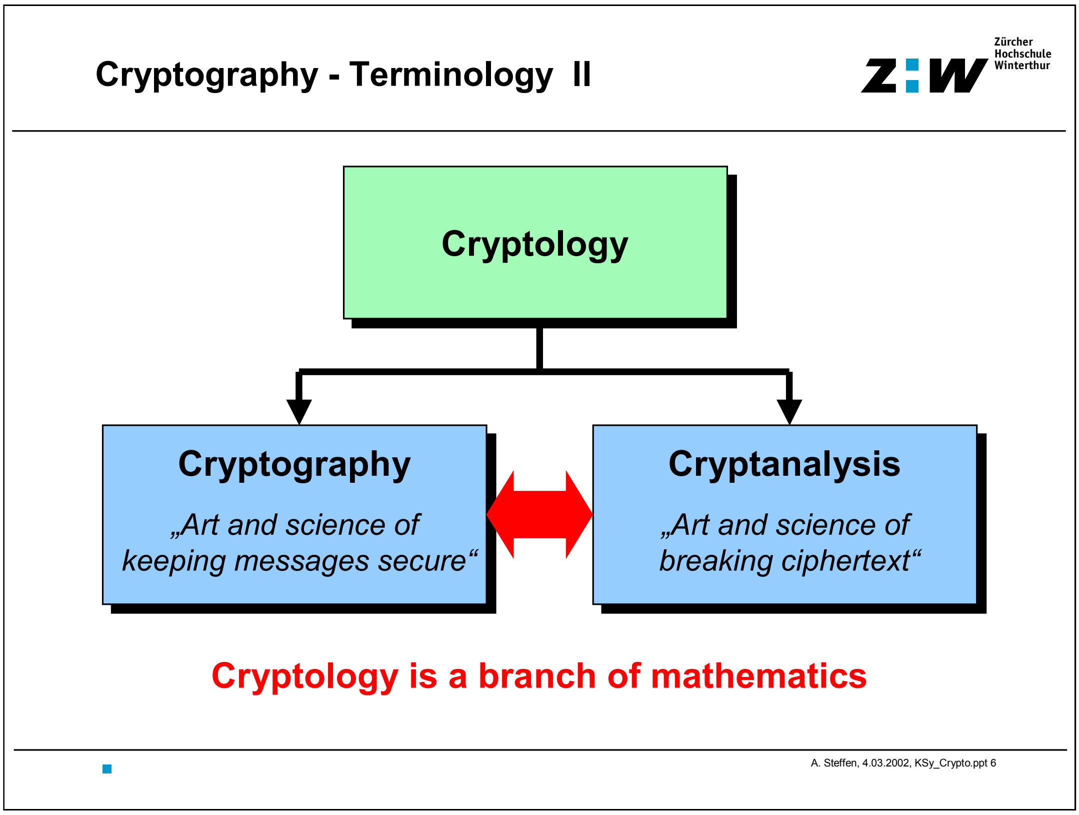
Messages and Encryption

- A message is **plaintext** (sometimes called cleartext). The process of disguising a message in such a way as to hide its substance is called **encryption**.
- An encrypted message is **ciphertext**. The process of turning ciphertext back into plaintext is called **decryption**.

Algorithms and Keys

- A **cryptographic algorithm**, also called a **cipher**, is the mathematical function used for encryption and decryption.
- The security of a modern cryptographic algorithm is based on a secret **key**. This key might be any one of a large number of values. The range of possible key values is called the **keyspace**.
- Both encryption and decryption operations are dependent on the key K and this is denoted by the K subscript in the functions $E_K(P) = C$ and $D_K(C) = P$

Source: Bruce Schneier, „Applied Cryptography“, Second Edition, pp. 1..3,
John Wiley & Sons, 1996



Cryptography - Terminology II

Zürcher Hochschule Winterthur

Cryptology

Cryptography

„Art and science of keeping messages secure“

Cryptanalysis

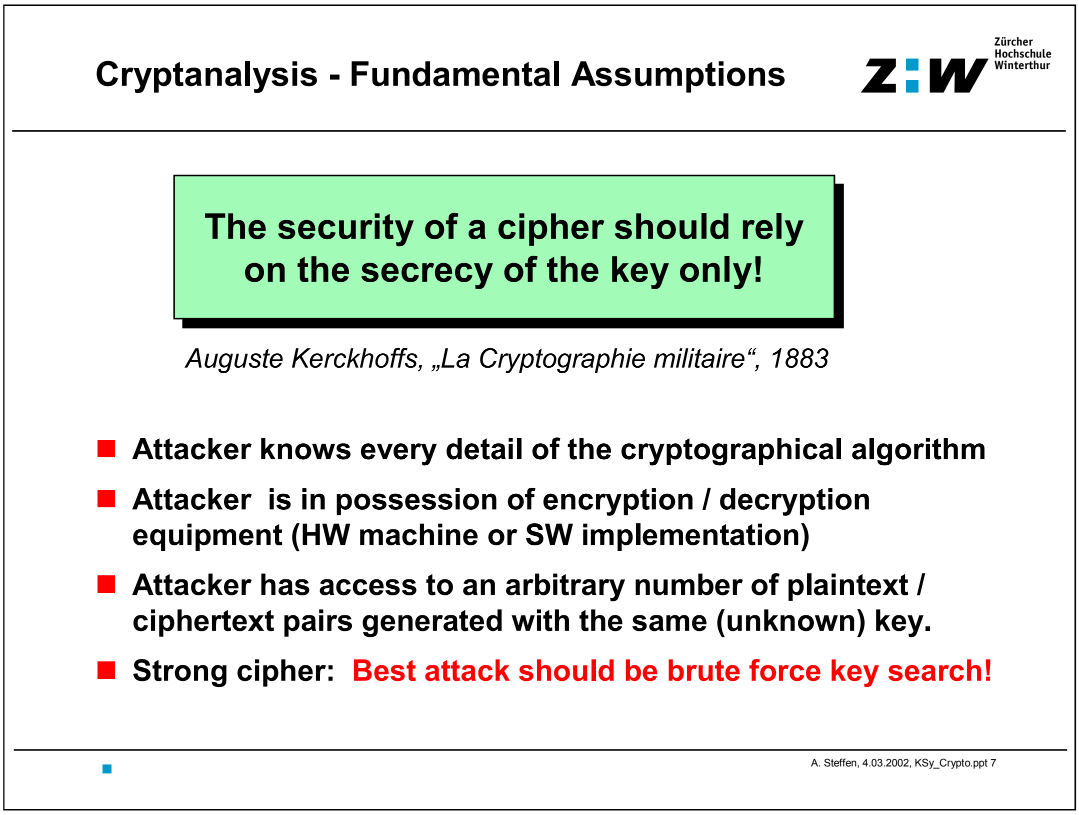
„Art and science of breaking ciphertext“

Cryptology is a branch of mathematics

Cryptology

- The art and science of keeping messages secury is **cryptography**, and it is practiced by **cryptographers**.
- **Cryptanalysts** are practitioners of **cryptanalysis**, the art and science of breaking ciphertext; that is seeing through the disguise.
- The branch of mathematics encompassing both cryptography and cryptanalysis is **cryptology** an its practitioners are **cryptologists**.
- Modern cryptologists are generally trained in **theoretical mathematics** – they have to be.

Source: Bruce Schneier, „Applied Cryptography“, Second Edition, p. 1,
John Wiley & Sons, 1996



Cryptanalysis - Fundamental Assumptions

The security of a cipher should rely on the secrecy of the key only!

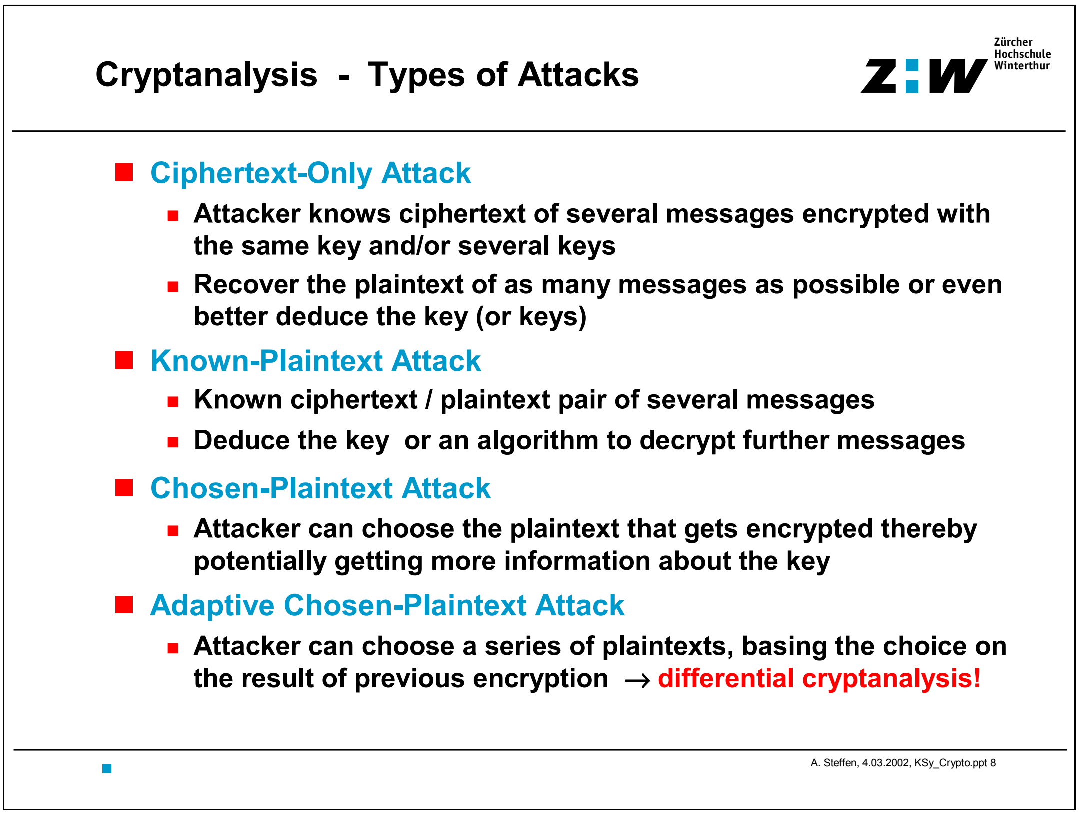
Auguste Kerckhoffs, „La Cryptographie militaire“, 1883

- **Attacker knows every detail of the cryptographical algorithm**
- **Attacker is in possession of encryption / decryption equipment (HW machine or SW implementation)**
- **Attacker has access to an arbitrary number of plaintext / ciphertext pairs generated with the same (unknown) key.**
- **Strong cipher: Best attack should be brute force key search!**

„La Cryptographie militaire“

- Author: Auguste Kerckhoffs, born 1835 at Nuth, Holland
- **Good cryptographic algorithms are found only through thorough cryptanalysis!**
- Kerckhoffs deduced the following **six requirements** for selecting usable field ciphers:

1) the system should be, if not theoretically unbreakable, unbreakable in practice
2) Compromise of the system should not inconvenience the correspondents
3) The key should be remembrable without notes and should be easily changeable
4) The cryptograms should be transmissible by telegraph
5) the apparatus or documents should be portable and operable by a single person
6) the systems should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.



Cryptanalysis - Types of Attacks

- **Ciphertext-Only Attack**
  - **Attacker knows ciphertext of several messages encrypted with the same key and/or several keys**
  - **Recover the plaintext of as many messages as possible or even better deduce the key (or keys)**
- **Known-Plaintext Attack**
  - **Known ciphertext / plaintext pair of several messages**
  - **Deduce the key or an algorithm to decrypt further messages**
- **Chosen-Plaintext Attack**
  - **Attacker can choose the plaintext that gets encrypted thereby potentially getting more information about the key**
- **Adaptive Chosen-Plaintext Attack**
  - **Attacker can choose a series of plaintexts, basing the choice on the result of previous encryption → differential cryptanalysis!**

Differential Cryptanalysis

- Introduced in 1990 by Eli Biham and Adi Shamir, who used it to show that for certain classes of cryptographic algorithms an adaptive chosen plaintext attack existed that was much more efficient than brute force.
- Although potentially vulnerable, the „Data Encryption Standard“ (DES) was shown to be surprisingly resistant to differential cryptanalysis.

  - Why do the S-boxes contain exactly those optimal values that make such a differential attack as difficult as possible?
  - Why does DES use exactly 16 rounds, the minimum required to make the effort for differential cryptanalysis about the same as a brute force approach?

  Answer: Because in the early 1970s the developers at IBM already knew about differential cryptanalysis!

  IBM‘s Don Coppersmith wrote in 1992:

  > *The design took advantage of certain cryptanalytic techiques, most prominently the technique of „differential cryptanalysis“, which were not known in the published literature. After discussions with the National Security Agency (NSA), it was decided that disclosure of the design considerations would reveal the technique of differential cryptanalysis, a powerful technique that can be used against many ciphers. This in turn would weaken the competitive advantage the United States enjoyed over other countries in the field of cryptography*

National Security Agency (NSA)

- Created in 1952 by President Harry Truman with the mandate to listen in on and decode all foreign communications of interest to the security of the United States.
- Rumored to employ about 16‘000 people, among them about 2000 of the world‘s best mathematicians.

How to construct a Secure Cipher?

World War II German Enigma Machine

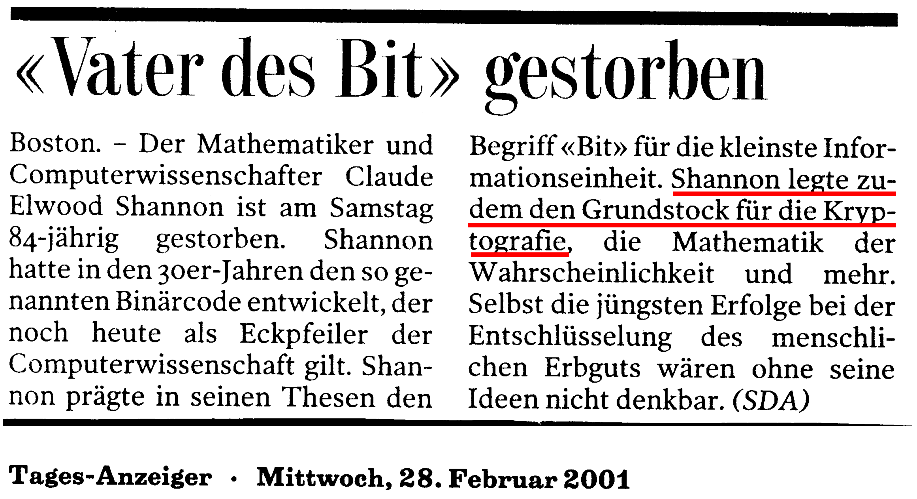
```
1 0 1 0 0 1 1 1 0 1 ...
```

Thomas Jefferson‘s Cipher Wheel

Claude Shannon 1916 - 2001

The Father of Information Theory

Zürcher Hochschule Winterthur



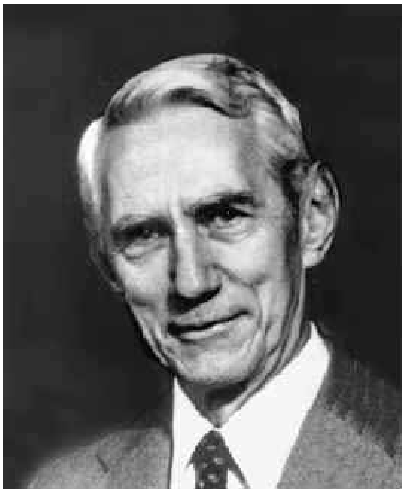
«Vater des Bit» gestorben

Boston. – Der Mathematiker und Computerwissenschafter Claude Elwood Shannon ist am Samstag 84-jährig gestorben. Shannon hatte in den 30er-Jahren den so genannten Binärcode entwickelt, der noch heute als Eckpfeiler der Computerwissenschaft gilt. Shannon prägte in seinen Thesen den Begriff «Bit» für die kleinste Informationseinheit. Shannon legte zudem den Grundstock für die Kryptografie, die Mathematik der Wahrscheinlichkeit und mehr. Selbst die jüngsten Erfolge bei der Entschlüsselung des menschlichen Erbguts wären ohne seine Ideen nicht denkbar. *(SDA)*

Tages-Anzeiger · Mittwoch, 28. Februar 2001

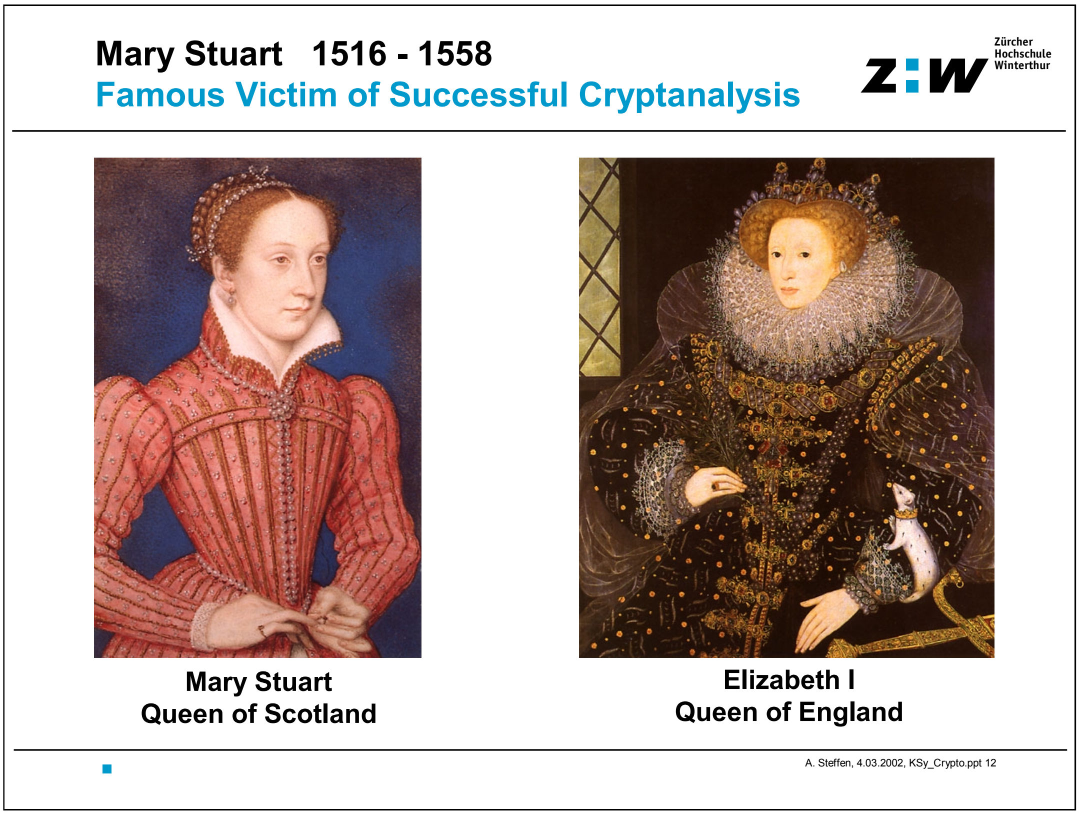
Claude Shannon 1916 - 2001
The Father of Information Theory

- Information Theory
  - Worked at MIT / Bell Labs
  - „The Mathematical Theory of Communication“ (1948)
  - Maximum capacity of a noisy transmission channel
  - Definition of the „binary digit“ (bit) as a unit of information
  - Definition of „entropy“ as a measure of information
- Cryptography
  - Model of a secrecy system
  - Definition of perfect secrecy
  - Basic principles of „confusion“ and „diffusion“



Basic Principles of „Confusion“ and „Diffusion“

- Throughout history the principles of „confusion“ and „diffusion“ have been used in innumerable codes and ciphers. Shannon was the first to formulate these two principles explicitely, „**confusion**“ standing for **substitution** operations and „**diffusion**“ standing for transposition or **permutation** operations. These two principles are still actively used in modern ciphers.



Mary Stuart 1516 - 1558

Famous Victim of Successful Cryptanalysis

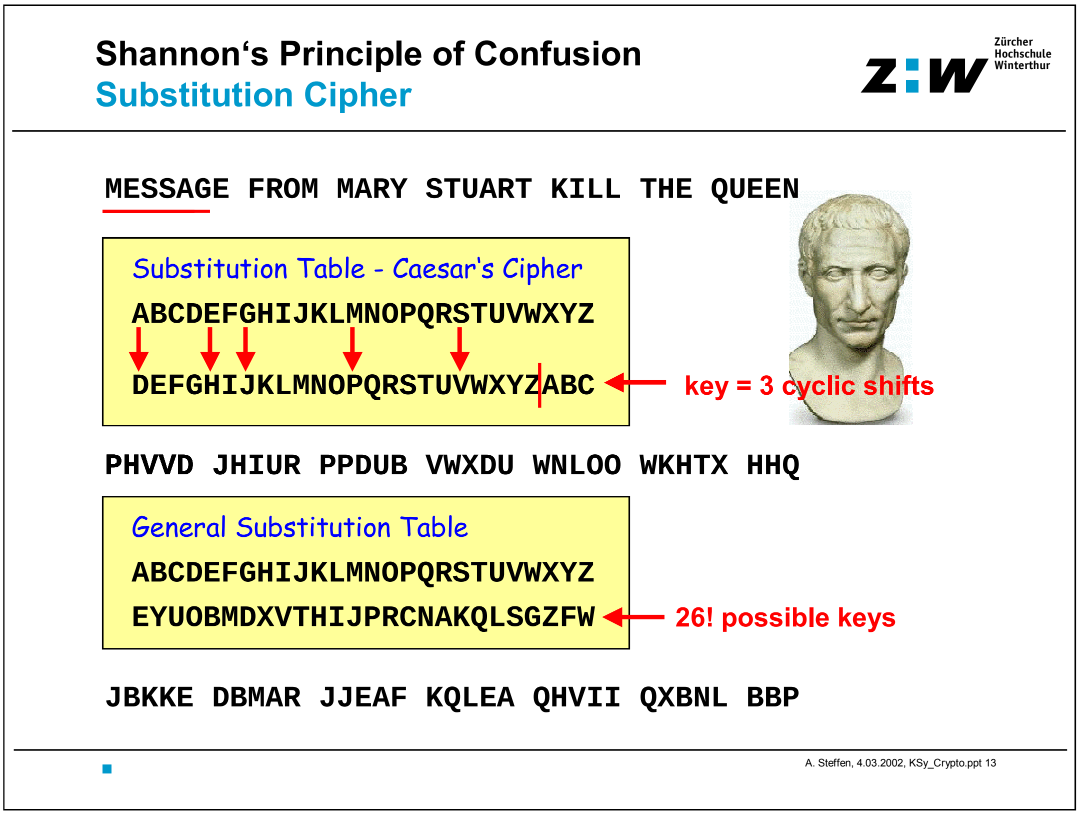
Mary Stuart
Queen of Scotland

Elizabeth I
Queen of England

Codes have decided the fates of empires throughout recorded history

- Mary Stuart, Queen of Scotland was put to death by her cousin Queen Elizabeth of England, for the high crime of treason after spymaster Sir Francis Walsingham cracked the secret code she used to communicate with her conspirators.

Source: Simon Singh, „The Code Book“, Doubleday, 1999



Shannon‘s Principle of Confusion

Substitution Cipher

```
MESSAGE FROM MARY STUART KILL THE QUEEN
```

Substitution Table - Caesar‘s Cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

key = 3 cyclic shifts

```
PHVVD JHIUR PPDUB VWXDU WNLOO WKHTX HHQ
```

General Substitution Table

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EYUOBMDXVTHIJPRCNAKQLSGZFW
```

26! possible keys

```
JBKKE DBMAR JJEAF KQLEA QHVII QXBNL BBP
```

Caesar Cipher

- The famous cipher used by Julius Caesar during his campaigns replaced each plaintext character by the character cyclicly shifted to the left.

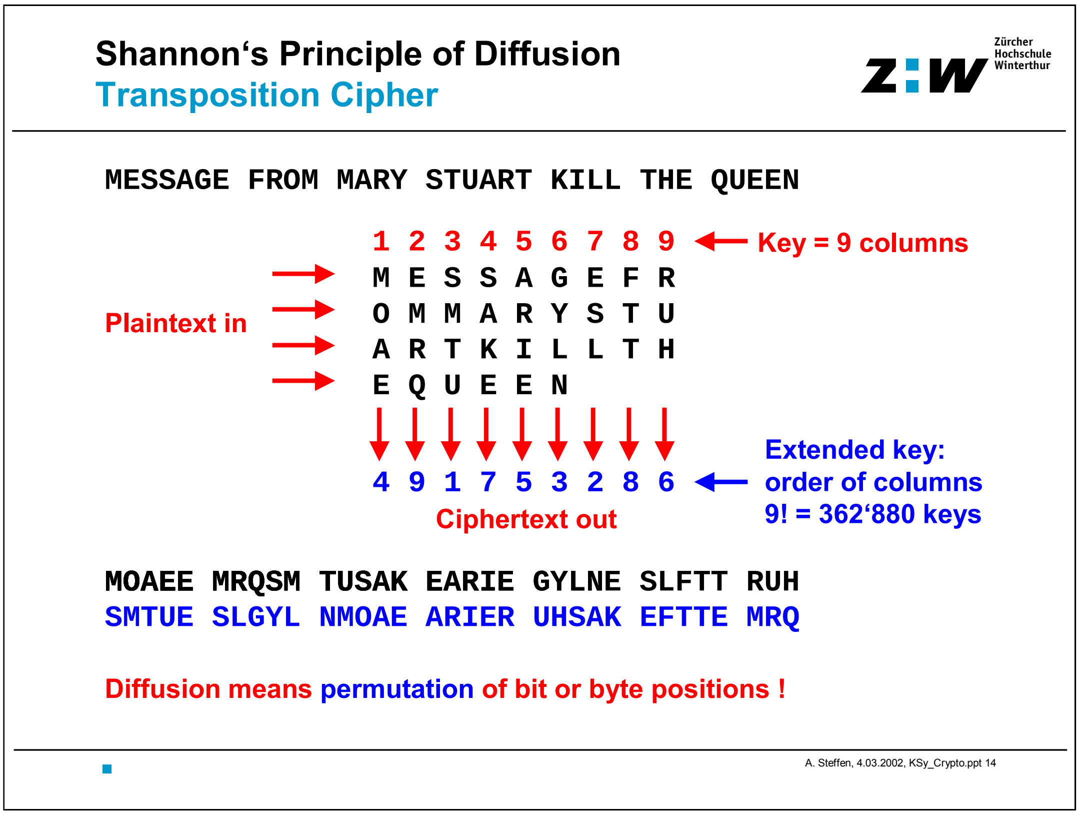
  “A“ is replaced by “D“, „B“ by „E“ and finally „Z“ by „C“.

  This is a simple **monoalphabetic substitution cipher,** where each character in an alphabet is replaced by another character in the same alphabet or sometimes even by a symbol of a different alphabet. With an alphabet of 26 characters and the most general substitution table there exist an enormous number of 26! different keys. This seems to make this system quite secure.

- Unfortunately monoalphabetic substitution schemes suffer from the severe drawback that with a given key, each occurence of a specific plaintext character is always mapped to the same ciphertext character, thus preserving the well-known character count statistics of natural language plaintexts, on the basis of which ciphertexts can be cracked quite quickly.

Substitution using S-Boxes

- In modern ciphers a fixed number of plaintext bits are grouped together and are substituted by a different bit combination according to a fixed lookup table.
- A software or hardware module which implements this substitution operation is called an **S-Box**.



Shannon‘s Principle of Diffusion
Transposition Cipher

MESSAGE FROM MARY STUART KILL THE QUEEN

Key = 9 columns

Plaintext in

```
1 2 3 4 5 6 7 8 9
M E S S A G E F R
O M M A R Y S T U
A R T K I L L T H
E Q U E E N
4 9 1 7 5 3 2 8 6
```

Ciphertext out

Extended key:
order of columns
9! = 362‘880 keys

MOAEE MRQSM TUSAK EARIE GYLNE SLFTT RUH
SMTUE SLGYL NMOAE ARIER UHSAK EFTTE MRQ

Diffusion means permutation of bit or byte positions !

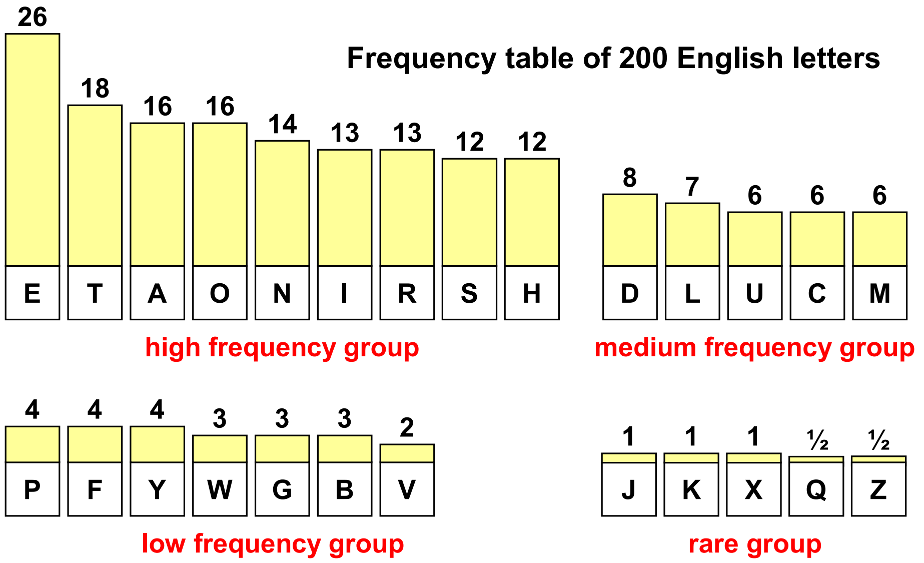
Classical Transposition Cipher

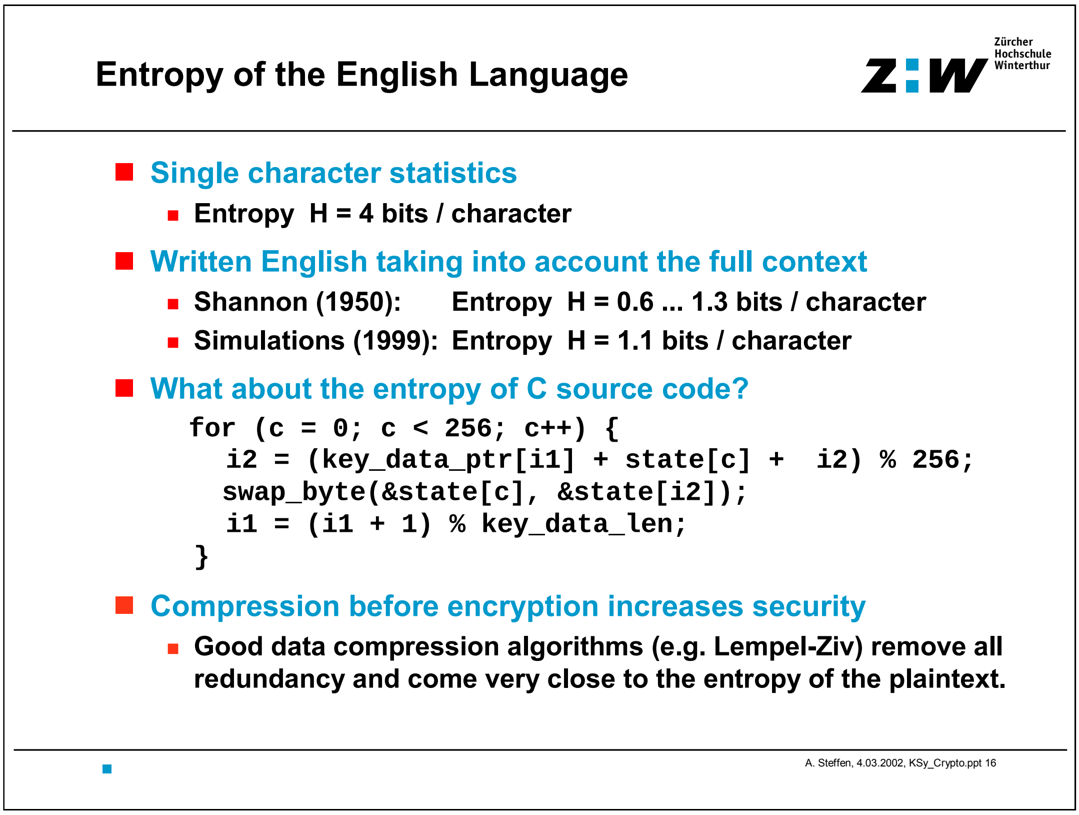
- In a classical transposition cipher the plaintext is written on a piece of paper in horizontal rows of *c* characters each. The number of columns *c* is part of the secret key. After the whole text has been written down in this fashion, the ciphertext is read out vertically column after column. In simpler versions this is done in increasing column order, but in a generalized method the columns could be chosen in any order (known of course by the authorized receiver) thereby extending the number of possible keys.

Permutation using P-Boxes

- In modern ciphers a fixed number of bits are written in linear order into a buffer and are read out in a permuted order controlled by a fixed lookup table.
- A software or hardware module which implements this permutation operation is called a **P-Box**.

Most Cryptoanalytic Attacks base on the
Redundancy of Natural Language Texts





Entropy of the English Language

- **Single character statistics**
  - **Entropy H = 4 bits / character**
- **Written English taking into account the full context**
  - **Shannon (1950): Entropy H = 0.6 ... 1.3 bits / character**
  - **Simulations (1999): Entropy H = 1.1 bits / character**
- **What about the entropy of C source code?**

```
for (c = 0; c < 256; c++) {
  i2 = (key_data_ptr[i1] + state[c] +  i2) % 256;
  swap_byte(&state[c], &state[i2]);
  i1 = (i1 + 1) % key_data_len;
}
```

- **Compression before encryption increases security**
  - **Good data compression algorithms (e.g. Lempel-Ziv) remove all redundancy and come very close to the entropy of the plaintext.**

Single Character Entropy

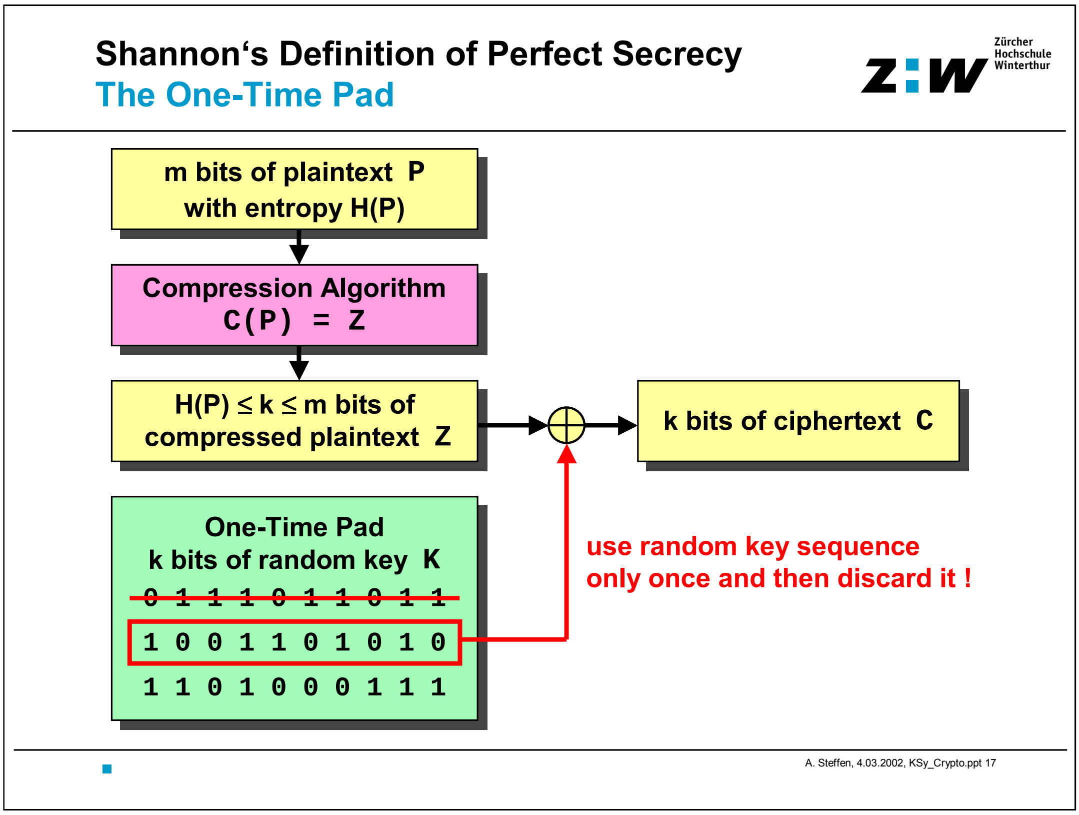
- By counting the number of occurences of each character c_i in a multitude of English texts the single character probabilities $p(c_i)$ can be determined. Over the whole alphabet these probabilities must add up to one.

$$\sum_{i=1}^{26} p(c_i) = 1$$

- The entropy can now be computed with the following formula

$$H = \sum_{i=1}^{26} p(c_i) \cdot \log_2 \frac{1}{p(c_i)}$$

- With the statistical values from the previous page the single character entropy becomes H = 4.19 bit, which is about half the 8 bit ASCII representation requires.



Shannon‘s Definition of Perfect Secrecy

The One-Time Pad

Zürcher Hochschule Winterthur

m bits of plaintext P
with entropy H(P)

Compression Algorithm
C(P) = Z

H(P) ≤ k ≤ m bits of
compressed plaintext Z

k bits of ciphertext C

One-Time Pad
k bits of random key K

~~0 1 1 1 0 1 1 0 1 1~~

1 0 0 1 1 0 1 0 1 0

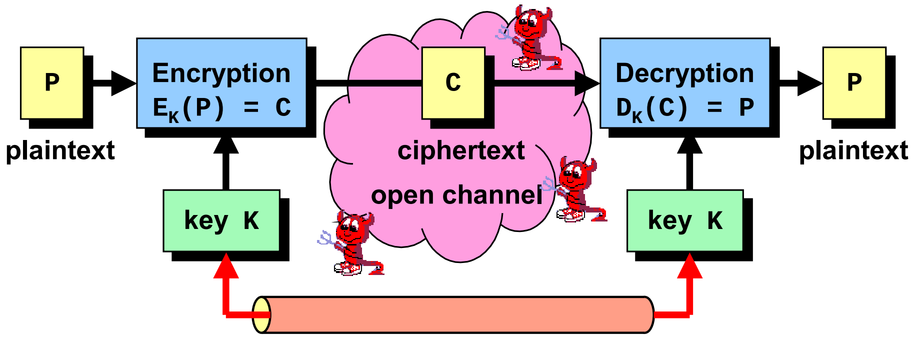
1 1 0 1 0 0 0 1 1 1

use random key sequence
only once and then discard it !

Perfect Secrecy

- Shannon has proven, that if correctly applied, the **one-time pad** becomes a **perfectly secure cryptosystem**.
- The plaintext is first reduced as close as possible to its true entropy by feeding it into a good compression algorithm. If ideal compression could be achieved, then changing any number of bits in the compressed message would result in another sensible message when uncompressed.
- The compressed plaintext is next XOR-ed bit-by-bit with random bits taken from the one-time pad, thus forming a perfectly random ciphertext. Once used these key bits must be discarded from the one-time pad and never used again.
- Without the correct key sequence it is impossible to retrieve the original plaintext since applying any other key of the same length would also give a sensible plaintext message after uncompression.
- **Why are one-time pads used only by secret agents and e-banking customers?** The secure distribution of the required keying material would pose an an enormous logistical problem if the one-time-pad were used on a large scale!

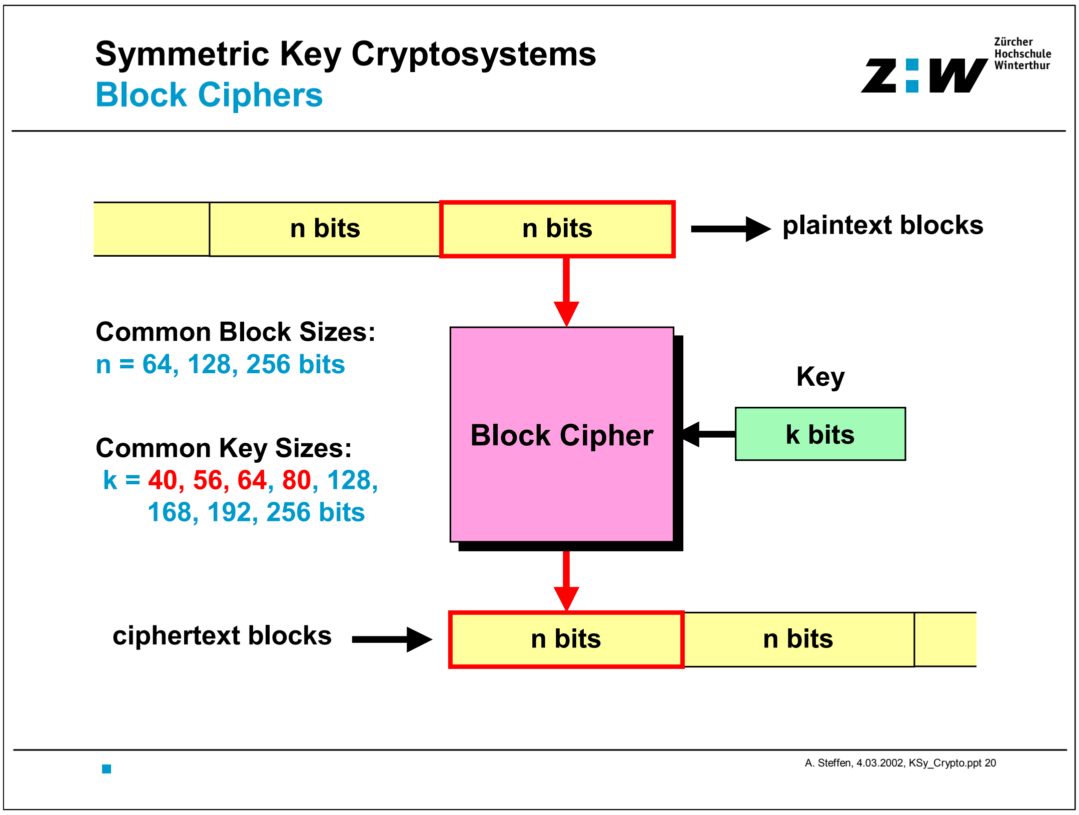
Shannon‘s Model of a Secrecy System
Symmetric or Secret-Key Cryptosystems



distribution of secret-key over secure channel

- Same key used for encryption and decryption
- Key must be kept absolutely secret
- Same key can be used for several messages, but should be changed periodically → secure key distribution problem!

Symmetric Key Cryptosystems
Block Ciphers



Symmetric Key Cryptosystems

Block Ciphers

n bits | n bits → plaintext blocks

Common Block Sizes:
n = 64, 128, 256 bits

Common Key Sizes:
k = 40, 56, 64, 80, 128,
168, 192, 256 bits

Block Cipher

Key

k bits

ciphertext blocks → n bits | n bits

Block Ciphers

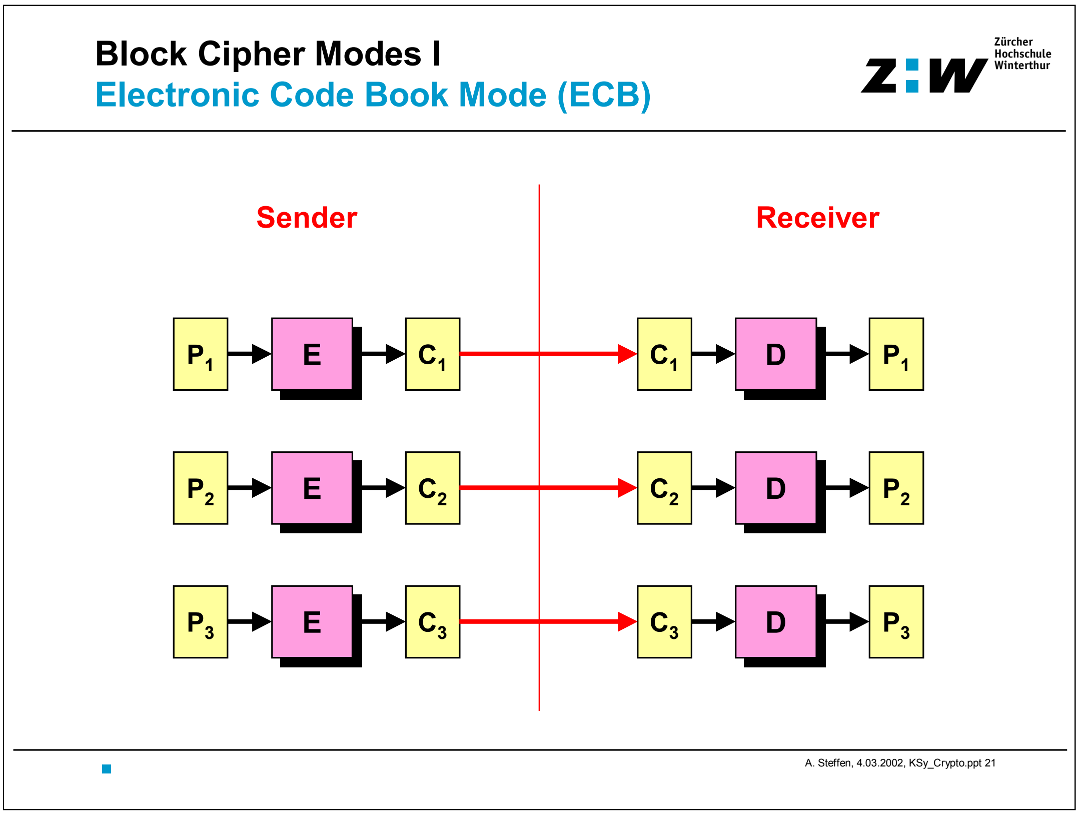
- A block ciphers cuts up a plaintext of arbitrary length into a series of blocks having a constant size of n bits. It then encrypts a single block of plaintext at a time and converts it into a block of ciphertext. In a good block cipher each of the n bits of the ciphertext block is a function of all n bits of the plaintext block and the k bits of the secret key.

Common Block Sizes

- Most block sizes currently are 64 bits but the trend is clearly going towards larger block sizes e.g. with the Advanced Encryption Standard (AES)

Common Key Sizes

- Key sizes with 40, 56 and 64 bits are clearly unsecure and should not be used anymore. To be on the safe side use a key size of 128 bits or more.

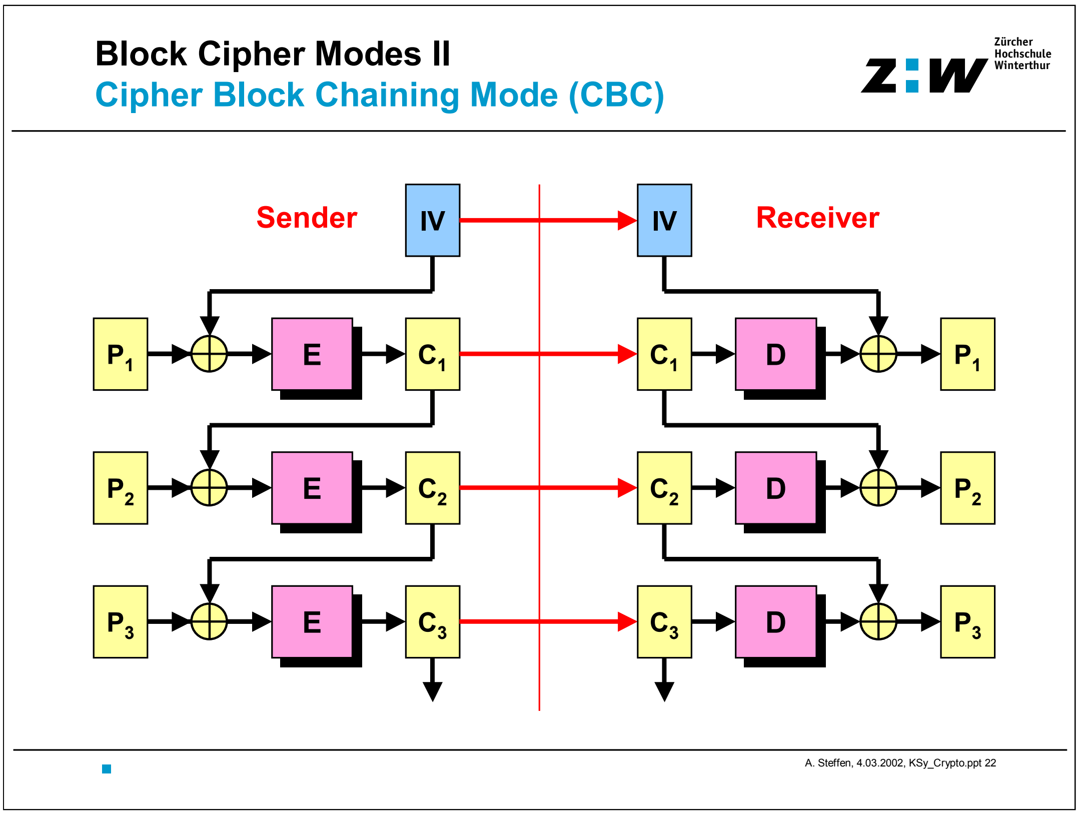


Block Cipher Modes I

Electronic Code Book Mode (ECB)

Electronic Code Book Mode (ECB)

- In ECB block cipher mode a plaintext input block is mapped statically to a ciphertext output block. With sufficient memory resources a lookup table or **Electronic Code Book** could be built, linking any ciphertext block pattern the ist corresponding plaintext block.
- Block ciphers in ECB mode are **vulnerable** to block **replay attacks**, because an opponent (without knowing the key) could replay an already transmitted ciphertext block at a later time if he thinks that the block contained e.g. an encrypted money transfer. If a session key is kept in use sufficiently long an attacker could also try to build a codebook of intercepted ciphertext blocks and guessed plaintext blocks.



Block Cipher Modes II

Cipher Block Chaining Mode (CBC)

Sender

Receiver

Cipher Block Chaining Mode (CBC)

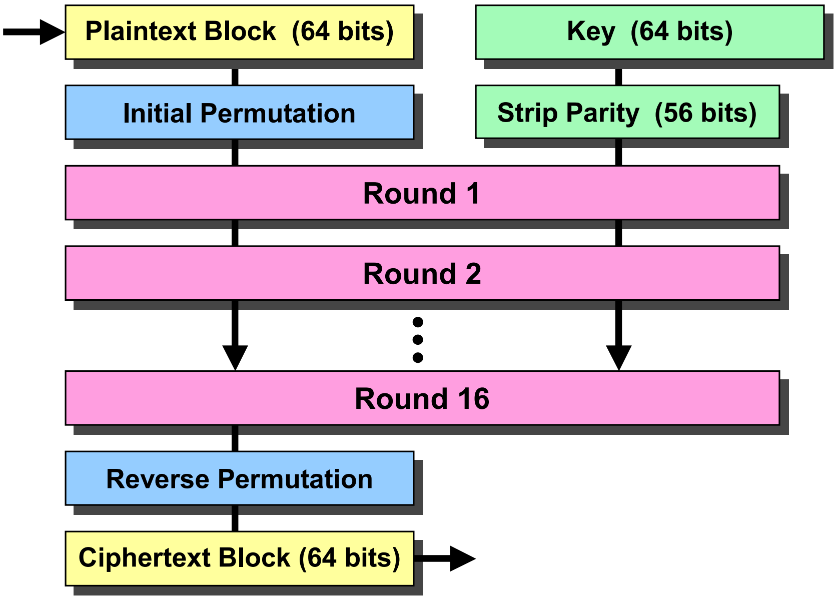
- In order to inhibit block replay attacks and codebook compilation, modern block ciphers are usually run in cipher block chaining mode. Each plaintext block is XOR-ed with the previous ciphertext block before encryption, so that identical plaintext blocks occuring in the same message show up as different ciphertext blocks.
- At the receiving side each block coming out of the decryption algorithm must first by XOR-ed with the previously received ciphertext block in order to recover the plaintext. A single bit error occuring over the transmission channel will result in the loss of one whole plaintext block plus a single bit error in the immediately following plaintext block. Error propagation is therefore restricted to two plaintext blocks.
- Any CBC-encrypted message must be initialized by an initialization vector (IV) that is openly transmitted over the insecure channel at the beginning of the session. In order to avoid replay attacks an IV value should be used only once and never be used again. This can be achieved either by assigning a monotonically increasing counter or a random value to the IV.

Block Ciphers
Present and Future Standards

Some Popular Block Ciphers

Name of Algorithm	Block Size	Key Size
DES (Data Encryption Standard, IBM)	64	56
Skipjack (NSA, clipper chip, was classified)	64	80
3DES (Triple DES)	64	168
IDEA (Lai / Massey, ETH Zürich)	64	128
CAST (Canada)	64	128
Blowfish (Bruce Schneier)	64	128 ... 448
RC2 (Ron Rivest, RSA)	64	40 ... 1024
RC5 (Ron Rivest, RSA)	64 ... 256	64 ... 256

Data Encryption Standard (DES)
Rounds of Confusion and Diffusion



Plaintext Block (64 bits)

Key (64 bits)

Initial Permutation

Strip Parity (56 bits)

Round 1

Round 2

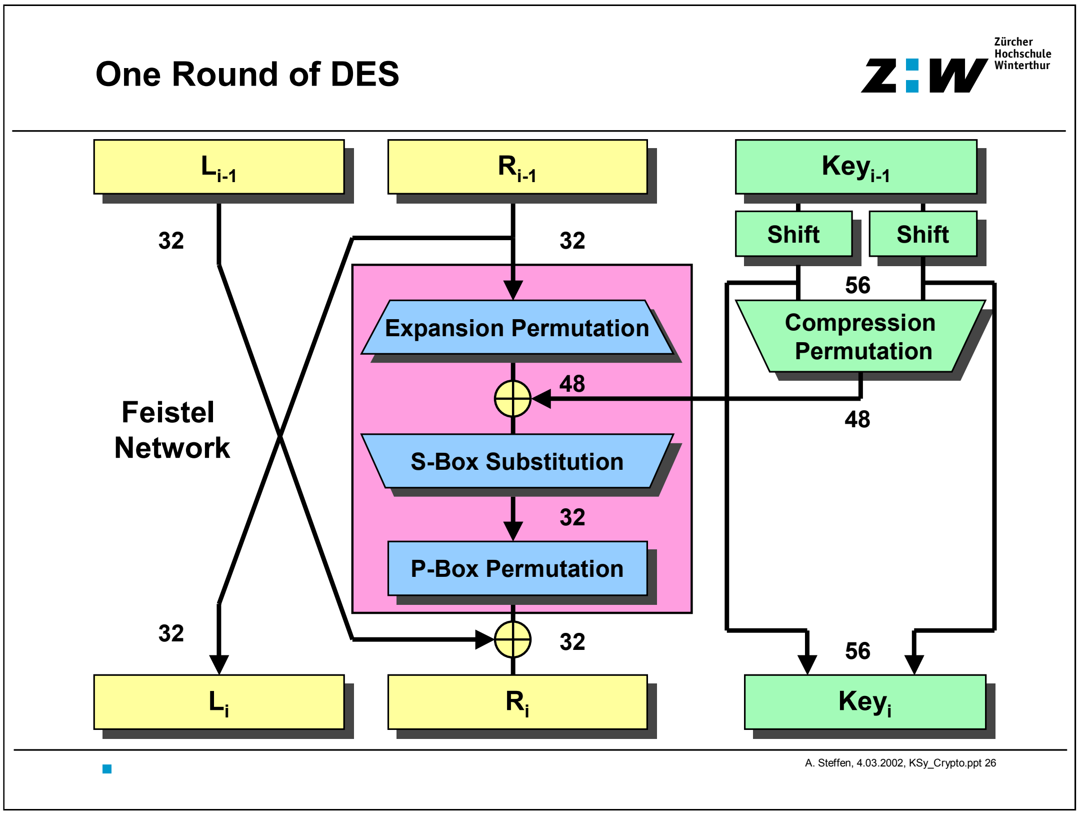
Round 16

Reverse Permutation

Ciphertext Block (64 bits)

Description of th Data Encrytion Standard (DES)

- The key length is 56 bits. (The key is usually written as a 64-bit number, but every eigth bit is used for parity checking and is discarded when the key is loaded into the DES algorithm.
- At ist simplest level, the algorithm is nothing more than a combination of the two basic techniques of encryption: confusion and diffusion. The fundamental building block of DES is a single combination of these techniques (a substitution followed) by a permutation) on the plaintext and based on the key. This is known as a **round**. DES has 16 rounds; it applies the same combination of techniques on the plaintext block 16 times. Any round less would make DES vulnerable to differential cryptanalysis!
- At the very beginning of the DES algorithm the 64 bit plaintext block is subjected to an initial permutation which does not depend on the key, whereas the inverse of this permutation finishes off the algorithm and delivers the ciphertext. These permutations do not affect the security of the DES algorithm and their purpose is not quite known.



One Round of DES

Zürcher Hochschule Winterthur

L_{i-1}

R_{i-1}

Key_{i-1}

32

32

Shift

Shift

56

Expansion Permutation

Compression Permutation

48

48

Feistel Network

S-Box Substitution

32

P-Box Permutation

32

32

56

L_i

R_i

Key_i

Feistel Networks

- At the heart of each DES round is a Feistel network, named after the IBM scientist Horst Feistel. The 64 bit block of incoming plaintext is split into a right and a left half of 32 bits each. Whereas the right half becomes the left half of the output text block at the end of the round, the left half enters a black box where it is first expanded to 48 bits by an expansion permutation and then XOR-ed with a 48-bit wide key. The resulting sum then enters an array of eight S-boxes with 6 input lines and 4 output lines each, producing a 32 bit wide output which then gets permuted by a P-box. The resulting output the black box is XOR-ed with the left half of the input text block and becomes the right half of the output text block.
- Each of the 16 DES rounds has a 48 bit key of ist own, derived by continually shifting and permuting the full 56 bit key from round to round.

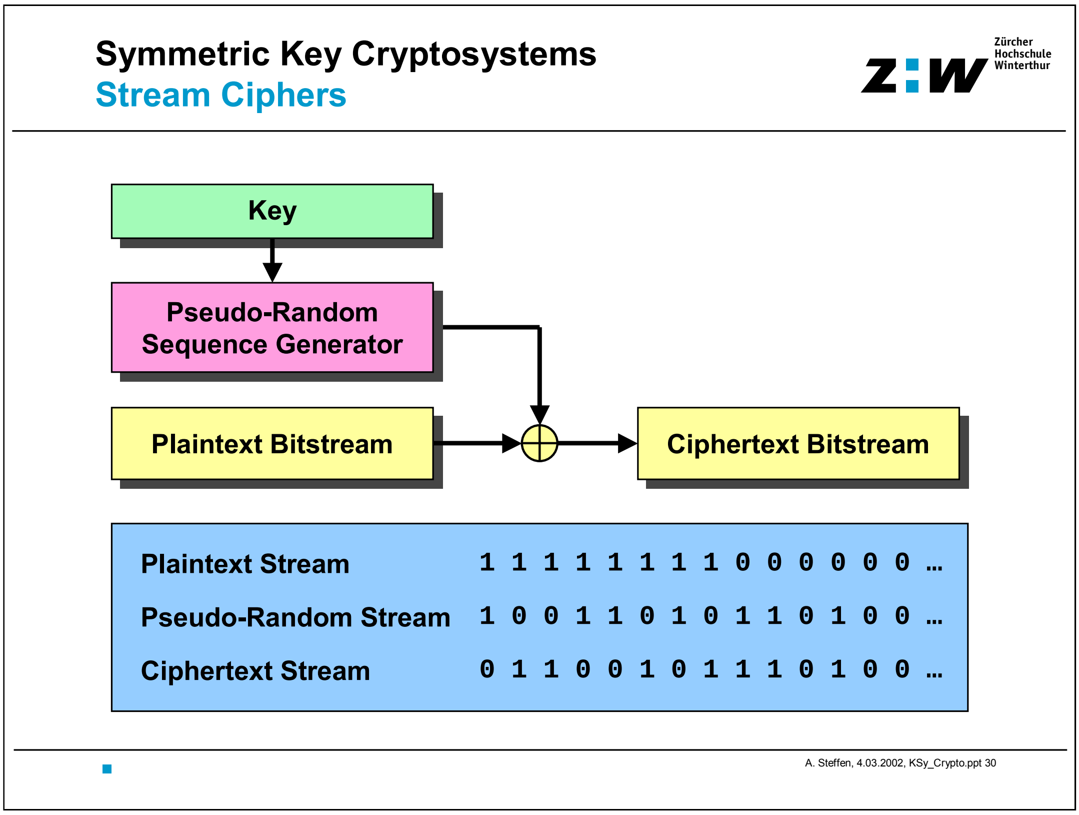
Advanced Encryption Standard (AES)
http://www.nist.gov/aes

- DES is nearly 25 years old!
  - Triple DES with a 168 bit key is the current Federal Information Processing Standard FIPS 46-3 (renewed in October 1999).
  - Single DES with 56 bit key is permitted for legacy systems only.
- Evaluation of an Advanced Encryption Standard
  - The National Institute of Standards and Technology (NIST, U.S. Department of Commerce) started a public contest in 1997.
  - Out of 5 final candidates Rijndael was chosen in October 2000.
- Requirements for AES
  - AES shall be publicly defined.
  - AES shall be a symmetric block cipher.
  - AES shall be implementable in both hardware and software.
  - AES shall be designed so that the key length may be increased as needed.
  - AES block size n = 128 bits, key size k = 128, 192, 256 bits

AES Finalists

- MARS (IBM)
  - Modified Feistel Network - 32 Rounds
  - Based on mixed structure DES
- RC6 (RSA)
  - Feistel Network - 20 Rounds
  - Based on modified RC5
- Twofish (Bruce Schneier)
  - Feistel Network - 16 Rounds
  - Based on modified Blowfish
- Serpent (Ross Anderson / Eli Biham / Lars Knudsen)
  - Substitution Permutation Network - 32 Rounds
  - Based on bitslice operations
- Rijndael (Joan Daemen / Vincent Rijmen)
  - Modified Substitution Permutation Network - 10 Rounds
  - Based on Square

Symmetric Key Cryptosystems
Stream Ciphers



Symmetric Key Cryptosystems
Stream Ciphers

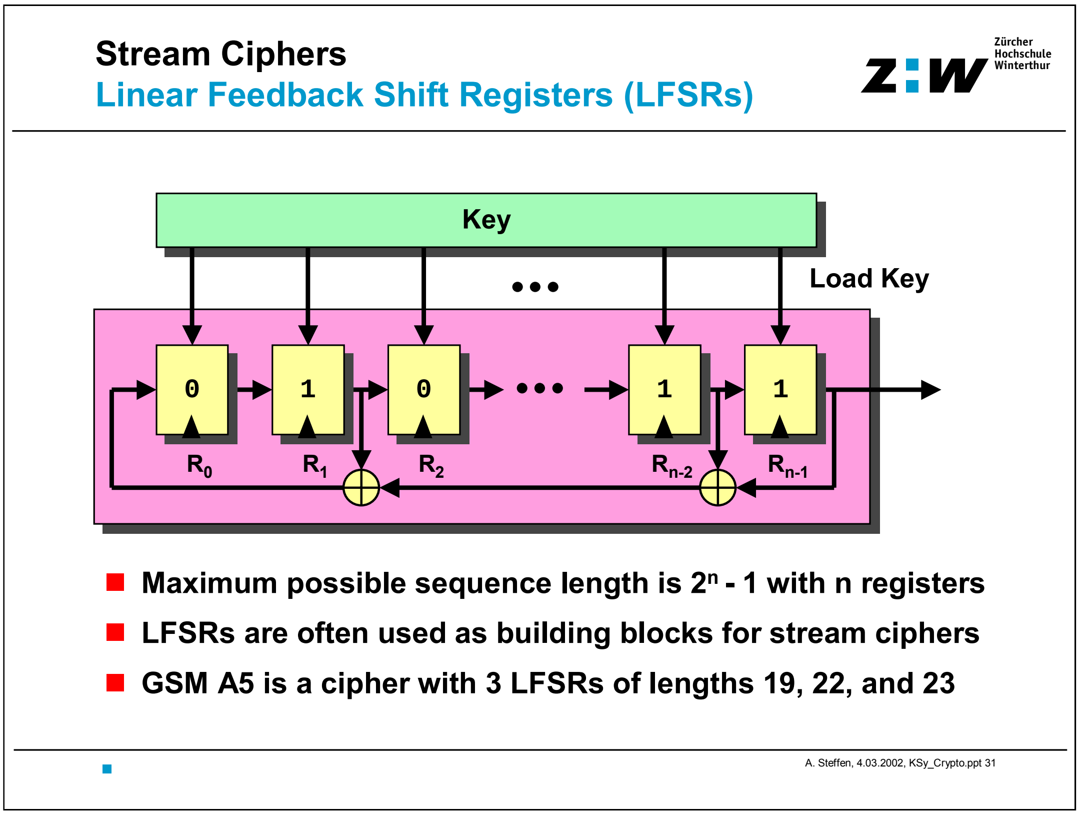
Plaintext Stream	1 1 1 1 1 1 1 1 0 0 0 0 0 0 …
Pseudo-Random Stream	1 0 0 1 1 0 1 0 1 1 0 1 0 0 …
Ciphertext Stream	0 1 1 0 0 1 0 1 1 1 0 1 0 0 …

Stream Ciphers

- Stream ciphers are based on a **key stream generator** that produces a **pseudo-random sequence** initialized by a **secret key**. This key stream is bit-wise XOR-ed with the plaintext bit stream, producing a ciphertext bit stream. At the receiver an identical key stream generator initialized with the same secret key is synchronized with the incoming ciphertext stream, . By combining the ciphertext stream and the synchronized key stream a single XOR at the receiver recovers the original plaintext.

Stream Ciphers versus Block Ciphers

- Stream ciphers usually work on a bit-level architecture and were traditionally implemented in dedicated hardware (ASICs). Very high throughputs can be achieved. Single bit errors in the ciphertext affect only a single plaintext bit and do not propagate.
- Block ciphers usually work on a word-level architecture and were traditionally implemented as software functions. Single bit errors propagate and affect two consecutive plaintext blocks in CBC mode.
- Today the boundaries between stream ciphers and block ciphers have been smeared somewhat. Stream ciphers can be used as block ciphers and vice versa. Modern stream ciphers often have word-sized internal registers and can be efficiently implented in software functions (e.g. RC4). Block ciphers have become faster and achieve high bandwidths.



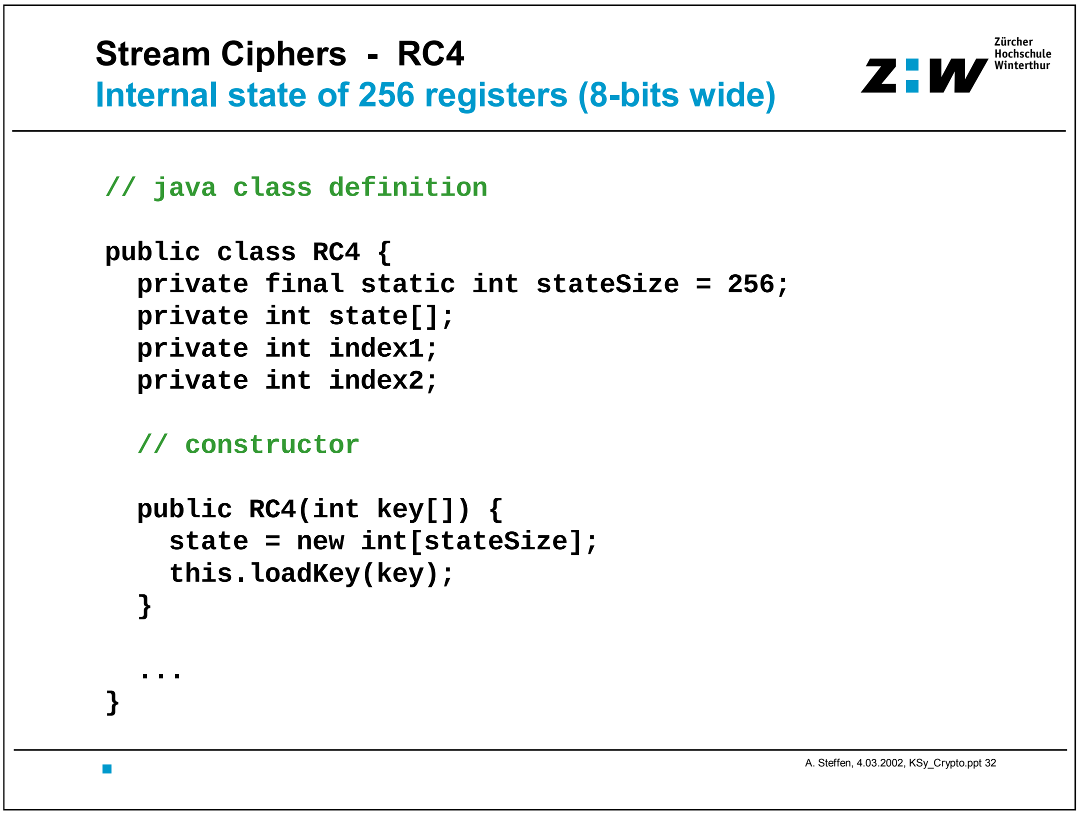
Stream Ciphers
Linear Feedback Shift Registers (LFSRs)

Zürcher Hochschule Winterthur

- Maximum possible sequence length is $2^n - 1$ with n registers
- LFSRs are often used as building blocks for stream ciphers
- GSM A5 is a cipher with 3 LFSRs of lengths 19, 22, and 23

Linear Feedback Shift Registers (LFSRs)

- Due to their finite state LFSRs themselves are very vulnerable to cryptanalysis. Only the artful combination of several LFSR building blocks with different lengths results in robust pseudo-random sources.
- The once powerful GSM A5 cipher containing three different LFSRs can nowadays be cracked in near real-time.



Stream Ciphers - RC4

Internal state of 256 registers (8-bits wide)

```
// java class definition

public class RC4 {
  private final static int stateSize = 256;
  private int state[];
  private int index1;
  private int index2;

  // constructor

  public RC4(int key[]) {
    state = new int[stateSize];
    this.loadKey(key);
  }

  ...
}
```

RC4 Stream Cipher

- RC4 invented by Ron Rivest was kept secret by RSA Data Security Inc. until the source code was anonymously leaked to a newsgroup in 1994. Restricted to 40 bit keys by U.S. export regulations until recently RC4 acquired an image of being unsecure. Nevertheless when used with 128 bit keys RC4 is still regarded as a secure and very elegant stream cipher by most experts.
- RC4‘s biggest advantage is its extremely simple, byte-oriented structure leading to extremely compact software implementations. RC4 possesses an internal state of 256 byte-wide registers which are initialized during startup by loading them with repeatedly concatenated versions of the secret key.

Stream Ciphers - RC4

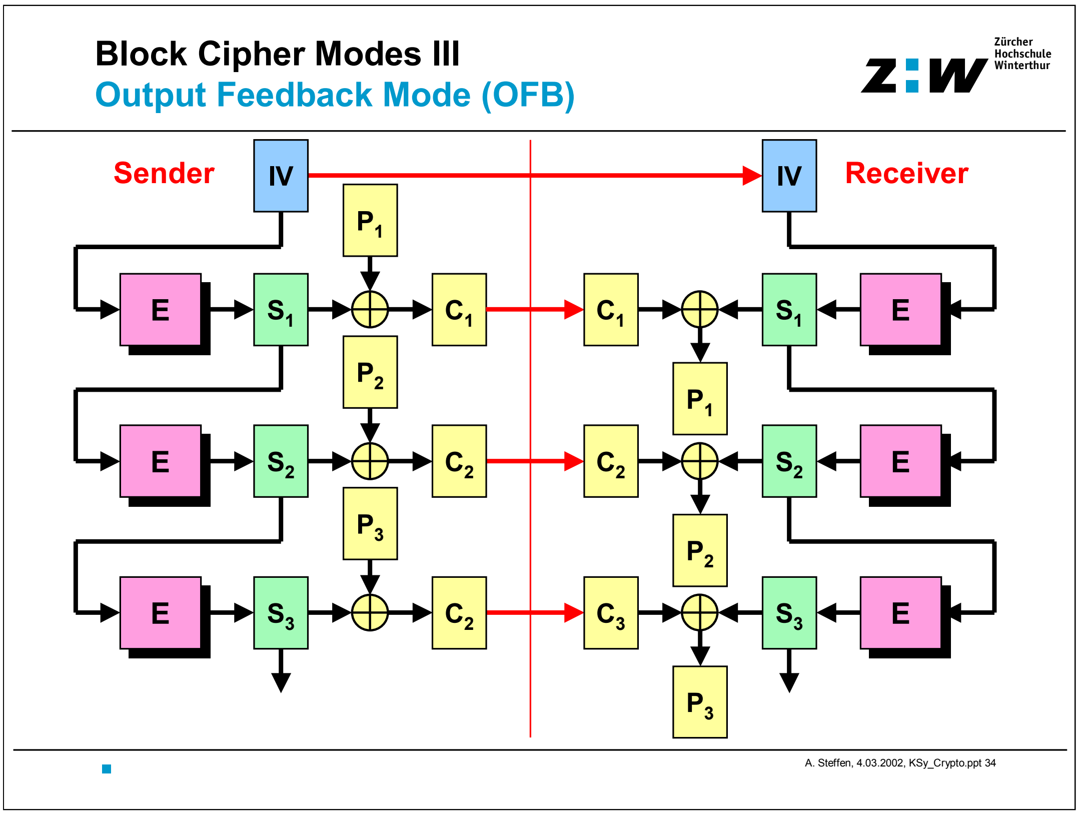
Simple state update by swapping registers

```
public void stream(int data[]) {
  int swap, xorIndex;

  for (int counter = 0; counter < data.length; counter++) {
    // compute next index
    index1 = (index1 + 1) % stateSize;
    index2 = (index2 + state[index1]) % stateSize;

    // swap contents of state[index1] and state[index2]
    swap = state[index1];
    state[index1] = state[index2];
    state[index2] = swap;

    // XOR state byte with data byte
    xorIndex = (state[index1] + state[index2]) % stateSize;
    int in = data[counter];
    data[counter] ^= state[xorIndex];
  }
}
```



Block Cipher Modes III

Output Feedback Mode (OFB)

Zürcher Hochschule Winterthur

A. Steffen, 4.03.2002, KSy_Crypto.ppt 34

Output Feed Back Mode (OFB)

- A block cipher in output feedback mode works as a key stream generator producing a pseudo-random key sequence a block at a time. By XOR-ing the key stream with the plaintext the block cipher actually works as a stream cipher.