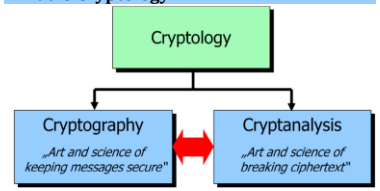
# Internetsicherheit - Einführung in die Kryptologie

## What is Cryptology?




## Goals of Cryptography

**Confidentiality (privacy)**
- A message can only be read by the intended parties

**Authentication**
- The receiver of a message can **ascertain its origin**, an attacker should **not be able to masquerade** as someone else

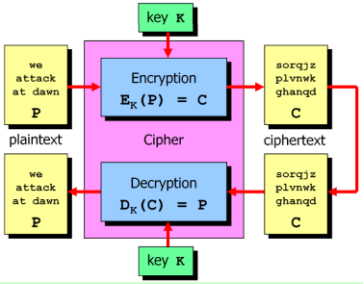
**Integrity**
- The receiver of a message can verify that the message was not altered in transit

**Non-Repudiation**
- The sender of a message cannot falsely deny later that he sent the message (the recipient can prove this to a third party)

**(Anonymity)**
- Not part of ISI

→ Form the basic building blocks for secure communication protocols!

## Secret Key Cryptography - Basic Terminology




**Primary goal**
- Confidentiality

**Messages and Encryption**
- A message is plaintext. The Process of disguising a message in such a way as to hide its substance is called **encryption**

**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**
- 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 $D_k(C) = P$
- Given a key, every possible plaintext must result in a unique ciphertext because otherwise, decryption would not be unambiguously possible

## What is a Secure Cryptographic Algorithm

**Ideal: the algorithm is information-theoretically secure**
- It cannot, by no means, be broken (even trying all keys does not help)
- There is only one such scheme known today: the One-Time Pad

**Desirable: the algorithm is computationally secure**
- It can be proven that there is no better method than trying all keys
- Today, there's no such algorithm known!

**Reality: we use algorithms we believe/hope to be close to computationally secure**
- The algorithm has been publicly available for a while (at least a few years)
- N one has found a way to break the algorithm significantly faster than trying all keys (at least not officially published!)
- Using all computers in the world, it takes a long time to try all keys
  - Trying all keys is also known as the **brute force attack**

## Computational Difficulty

- Cryptographic algorithms should have two properties
  - "Good Guys" (knowing the key) can compute the output efficiently
  - "Bad Guys" (without key) have a hard time to compute the correct output
- Analogy: Combination lock, three numbers between 1 and 20
  - $20^3 = 8000$ different combinations
  - 10 seconds to enter a combination → effort of the good guy
  - $8000 * 10 = 80000$ seconds = 1 day to try all combinations
  - On average: efford of the bad guy = 40'000 sec = 1/2 day
- What does a fourth number in the lock cost/help?
  - Good guy: 13.3 sec (+ 33%)
  - Bad guy: $\frac{1}{2} * 20^4 * 13.3 = 1066666$ sec = 12.5 days (+ 2400%)

→ **Making secrets/keys longer is usually a good idea!**

- Modern computers can try keys much faster than humans entering numbers in a combination lock
  - trying hundreds of thousands of keys per seconds is feasible
  - special hardware, parallelization to speed it up
- Today's ciphers use binary keys, **128 bits is considered secure**
  - $2^{128} = 3.4 * 10^{38}$
  - 1 Computer, 1000000 keys/s → $3.4 * 10^{32}$ sec = $10^{25} years$
  - Using 1000000 computers in parallel → $10^{19} years$
  - Compare: age of the universe is $1.5 * 10^{10} years$
- Are 64-bit keys also enough?
  - NO!
  - $2^{64} = 1.8 * 10^{19}$, $1000000 \frac{keys}{s} \rightarrow 1.8 * 10^{13}$ sec = $570000\ years$
  - 1000000 computers in parallel → 0.57 years = 208 days

## 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 cryptographic algorithm
- Attacker is in possession of encryption / decryption equipment
- Attacker has access to an arbitrary number of plaintext / ciphertext pairs generated with the same (unknown) key
- **Strong cipher:** There is no better attack than trying all keys (brute force attack)

**Types of attack**

**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 and can thereby potentially get more information about the key (one application: differential cryptanalysis)

→ **A strong cipher should resist all these attacks!**

## Historical Development of Cryptology

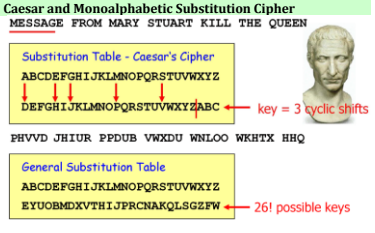
**Classical phase until 18th century**
- Various forms of message hiding (Steganography), e.g. tattoos on the scalps of slaves covered by hair
- Caesar cipher
- Mono- and polyalphabetic substitution ciphery
- Transposition ciphers

**"Semi"-modern phase (1800-1970)**
- Mechanization of ciphers, rotors machines

**Modern phase (1970-today)**
- Heavily influenced by Claude Shannon's work
- Computer-based ciphers, partially based on mathematical foundations (especially public key cryptography)

## Classical Phase

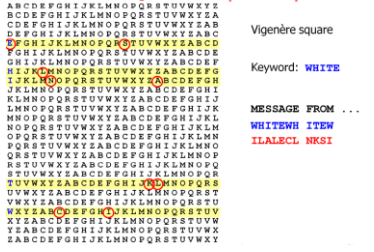
**Caesar and Monoalphabetic Substitution Cipher**



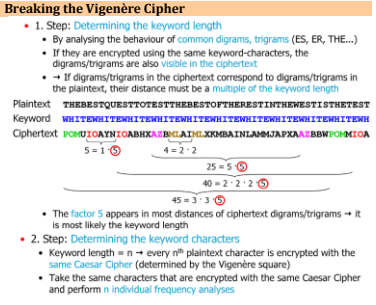

Substitution means replacing of bits or bytes using a table!

**Security of the Monoalphabetic Substitution Cipher**
- Used in the Arab world and Europe (alchemists, monks, diplomats) as early as during the 13th century
- $26! = 4 * 10^{26} = 2^{88} Keys$ → Brute force attack even today infeasible
- But: the cipher is very susceptible to frequency analysis
  - A specific plaintext character is always mapped to the same ciphertext character
  - Cryptanalysis: compare the frequencies of occurrence of the ciphertext characters with the character-frequencies of the plaintext-language
- The cipher (and variants) was used for centuries, only a few scientists were able to break the cipher back then

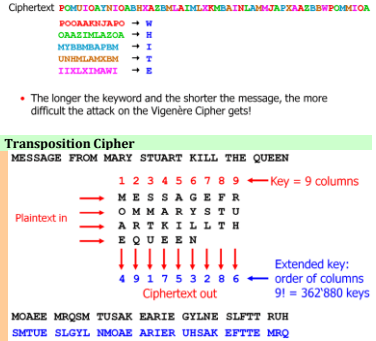
**Vigenère Polyalphabetic Substitution Cipher (1553)**




**Breaking the Vigenère Cipher**

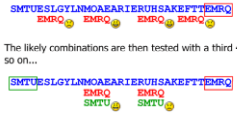



**Transposition Cipher**




Transposition means permutation of bit- or byte-positions!

**Breaking the Transposition Cipher**
- Trick: the cipher can be attacked „incrementally"
  - The attacker first guesses the number of columns (here: 9)
  - 33 characters / 9 = 3.66 → 6 columns with 4 characters and 3 columns with 3 characters
  - He then takes a 4-character block from the ciphertext and compares it with all other 4-character blocks
  - If "4 reasonable 2-character combinations" show up, then it is likely that the columns follow after each other in the column-ordered plaintext




  - The likely combinations are then tested with a third 4-character block and so on...




## Semi-Modern Phase

- Desire to increase speed to encrypt / decrypt → mechanical ciphers (usually rotor machines)
- Cryptography became even more important with the advent of radio communications, especially for the military
- First mechanical cipher: Thomas Jefferson's Cipher Wheel

**World War II: German Enigma Machine**
- Electromechanical rotor machine implementing a polyalphabetic substitution cipher
- Used during World War II by the German Wehrmacht and Kriegsmarine to encrypt most of its communications
- Key determines initial rotor settings and cables on the plugboard, $10^{23}$ possible Keys (= 76 Bits)
- Key was kept constant for a day, distributed via codebooks
- Could be broken by the British at Bletchley Park, mainly due to weaknesses both in the implementation and the usage of the machine

## Modern Phase

**Scientific Foundations by Claude Shannon (1916-2001)**
- Worked at MIT / Bell Labs
- Information Theory
  - 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
  - Formulation the basic principles of "confusion" (substitution operations) and "diffusion" (transposition/permutation operations)

## Entropy - the Measure of Information

- Shannon defines entropy as the amount of information in the outcome of a random experiment (e.g. rolling a dice), measured in bits
  - "the difficulty to guess the outcome correctly"
- For a discrete random experiment x with n possible outcomes (1...n), entropy is defines as follows

$$H = \sum_{i=1}^{n} p(i) log_2 \left(\frac{1}{p(i)}\right)$$

- p(i) is the probability of the outcome I and the probabilities of all outcomes must add up to one:

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

- The entropy of a discrete random experiment is always maximized if all outcomes are equally like

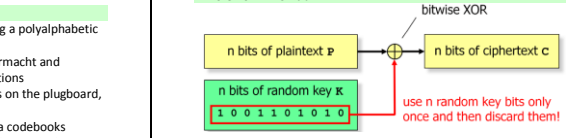
**Entropy and Key Length**
- Entropy of flipping a fair coin (pheads = ptails = 0.5)
  $H = \frac{1}{2} * log_2(2) + \frac{1}{2} * log_2(2) = 2 * \frac{1}{2} * log_2(2) = 1\ Bit$
- Entropy of flipping an unfair coin (pheads = 0.25, ptails = 0.75)
  $H = \frac{1}{4} * log_2(4) + \frac{3}{4} * log_2\left(\frac{4}{3}\right) = 0.81\ Bit$
- A property of entropy is that it is **additive**
  - Throwing two fair coins together:
    $H = 4 * \frac{1}{4} * log_2(4) = 2\ Bits$
    → equal to throwing two coins seperately (1 Bit + 1 Bit)
- So what's the entropy of a cryptographic key with length 128 Bits?
  - If the bits are selected independently and randomly: 128*1 = 128 Bits
  - but if the bits are not selected completely randomly, the entropy is smaller; with p = 0.25/0.75: 128 * 0.81 = 104 Bits (corresponds to a truly randomly selected key of 104 bits)
  - Since the second key has 24 Bits less entropy, it is $2^{24} = 16777216$ times easier to break than the first key with a brute force attack

→ **Selecting key material as randomly as possible is crucial in cryptography!**

**Entropy of the English Language**
- Cryptanalysis often bases on the **redundancy of natural language texts**
  → analysis with Shannon's measure of information
- If all 26 characters were equally frequent and selected independently
  - Entropy $H = 4.7 \frac{bits}{character}$ → no redundancy (max. entropy)
- With real probability distribution of characters in English texts
  - $H = 4.19 \frac{bits}{character}$ → 0.51 bits redundancy per 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
  → Logs and lots of redundancy in real English text!
- **Reducing this redundancy makes frequency analysis more difficult**
- How? → Compressing before encryption!
  - Good data compression algorithms (e.g. Lempel-Ziv) remove nearly all redundancy and come very close to the entropy of the plaintext

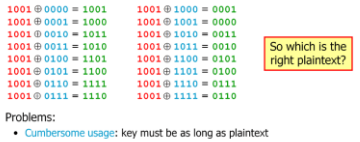
## Shannon's Definition of Perfect Security

**The One-Time Pad**



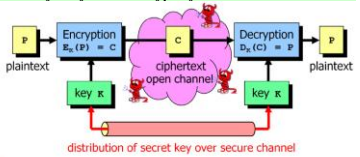

- Decrypting works by applying the same key sequence again
  $C = P \oplus K \rightarrow P = C \oplus K$
- This is the only cipher known today that is **information theoretically secure** → even trying all keys won't work!
- Why?
  - With a ciphertext of length n, trying all $2^n$ keys results in all $2^n$ different possibilities of the plaintext of length n
  - The attacker cannot tell which plaintext is the correct one

- Example: Plaintext = 0010, Key = 1011
  Resulting Ciphertext: 0010 ⊕ 1011 = 1001
- The attacker intercepts the ciphertext and performs a brute force attack: P = C ⊕ K




- Problems:
  - Cumbersome usage: key must be as long as plaintext
  - Only used in situations with extreme security demands (military etc.)

**Secret Key or Symmetric Cryptosystems**




- 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!

## Summary

- **Cryptology** = Cryptography + Cryptanalysis
- **Goals**: confidentiality, authentication, integrity, non-repudiation
- Secret key cryptosystem: a message (plaintext) is encrypted using a **cipher** and a secret key and results in the corresponding ciphertext
- **128 bits** is a reasonable key-length for secret key cryptosystems
- All security should lie in the **secrecy of the key**
- Basic operations of ciphers
  - **Substitution** (diffusion) means replacing of bits using a table
  - **Transposition** (confusion) means permutation of bit- or byte-positions
- Cryptosystems can often be broken because of redundancy of the plaintext → **frequency analysis**
- Claude Shannon started the area of modern cryptography
  - **Entropy** as the measure for information
  - One-Time-Pad as the **perfect cryptosystem**
  - General model of **secret key cryptosystems**