IKT-Sicherheit

Kryptographie und Kryptoanalyse

Paul Lackner

15. September 2025

1. Grundlagen
   - Terminologie Kryptographie und Kryptoanalyse
   - Grundlagen Kryptographie
   - Zusammenfassung
2. Symmetrische Kryptographie
   - Erste Anfänge der Kryptographie
   - Moderne symmetrische Kryptographie
   - Block und Stromchiffren
   - Advanced Encryption Standard (AES)
   - One-Time-Pads (OTP)
   - Zusammenfassung
3. Asymmetrische Kryptographie
   - Grundlagen und Geschichte
   - Diffie-Hellman (DH)
   - Diskreter-Logarithmus-Problem (DLP)
   - Rivest-Shamir-Adelman (RSA)
   - Digitale Zertifikate

Kontakt

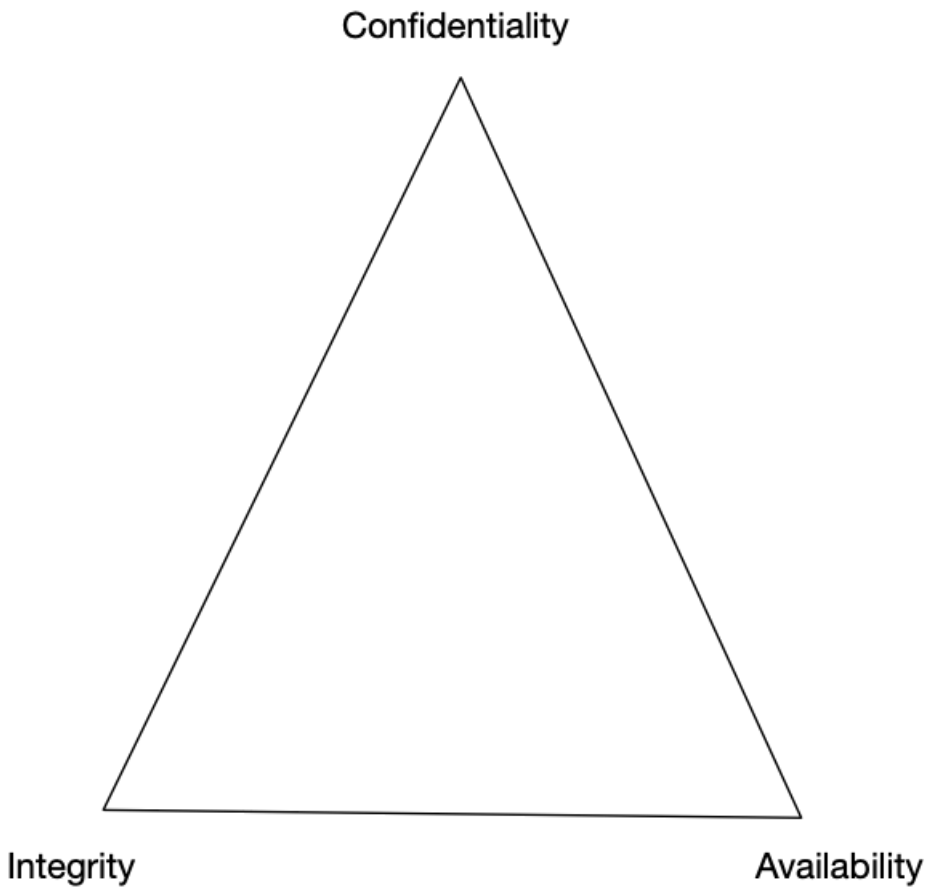
- Email: Auf der Tafel bzw. bei `https://lithilion.at`
- Matrix: @Lithilion:fairydust.space

Grundlagen

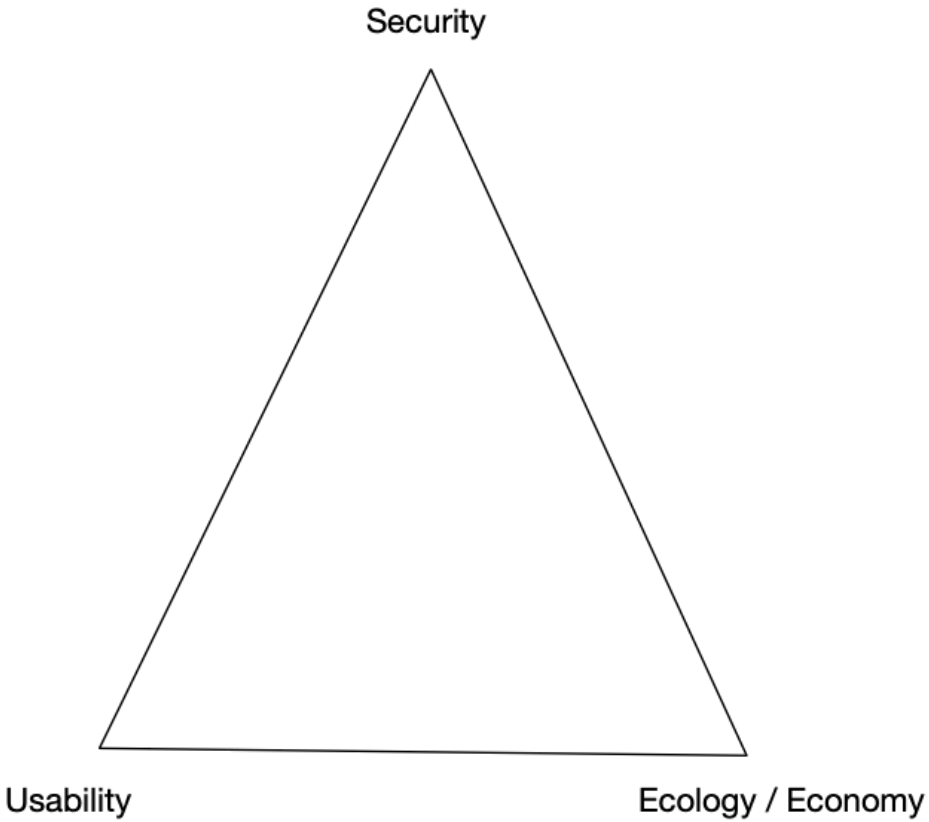
Was ist Kryptographie?

- Verbergen und Verschleiern von Daten
- Zugriffsschutz
- Veränderungsschutz
- Mathematik und Algorithmen

Schutzziele der IT/Information-Security

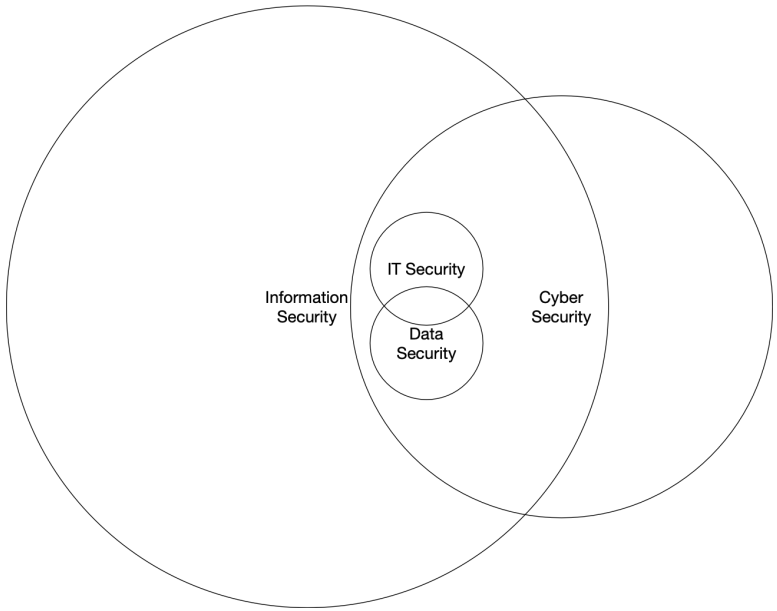


Schutzziele der IT/Information-Security



\w+ Security

- Data Security
- IT-Security
- Information Security
- Cyber Security



CIA - Übung

Schutzziele

Welche Schutzziele verletzen die folgenden Angriffe?

Verfügbarkeit | Integrität | Vertraulichkeit

CIA - Übung

Schutzziele

Welche Schutzziele verletzen die folgenden Angriffe?

Verfügbarkeit | Integrität | Vertraulichkeit

- (D)DoS

CIA - Übung

Schutzziele

Welche Schutzziele verletzen die folgenden Angriffe?

Verfügbarkeit | Integrität | Vertraulichkeit

- (D)DoS
- Passwort-Bruteforce

CIA - Übung

Schutzziele

Welche Schutzziele verletzen die folgenden Angriffe?

Verfügbarkeit | Integrität | Vertraulichkeit

- (D)DoS
- Passwort-Bruteforce
- Phishing

CIA - Übung

Schutzziele

Welche Schutzziele verletzen die folgenden Angriffe?

Verfügbarkeit | Integrität | Vertraulichkeit

- (D)DoS
- Passwort-Bruteforce
- Phishing
- Datendiebstahl

CIA - Übung

Schutzziele

Welche Schutzziele verletzen die folgenden Angriffe?

Verfügbarkeit | Integrität | Vertraulichkeit

- (D)DoS
- Passwort-Bruteforce
- Phishing
- Datendiebstahl
- (Remote)-Code-Execution

Was ist Kryptoanalyse?

- Aufbrechen der Kryptographie
- Finden von Fehlern und Schwachstellen in Algorithmen

Kerckhoffsche Prinzip

- Auguste Kerckhoff - 1883 La cryptographie militaire
- Open Source Prinzip der Algorithmen

Kerckhoffsche Prinzip

Es darf nicht der Geheimhaltung bedürfen und soll ohne Schaden in Feindeshand fallen können.

Kerkhoffsche Prinzip

1. Das System muss im Wesentlichen (...) unentzifferbar sein.
2. Das System darf keine Geheimhaltung erfordern (...).
3. Es muss leicht übermittelbar sein und man muss sich die Schlüssel ohne schriftliche Aufzeichnung merken können (...).
4. Das System sollte mit telegraphischer Kommunikation kompatibel sein.
5. Das System muss transportabel sein und die Bedienung darf nicht mehr als eine Person erfordern.
6. Das System muss einfach anwendbar sein (...).

Identitätsüberprüfung

Wie überprüfe ich Identitäten und Berechtigungen?

Erklärt mir die Begriffe Identifizierung, Authentifizierung und Authorisierung anhand einer Grenzkontrolle

Identitätsüberprüfung

Wie überprüfe ich Identitäten und Berechtigungen?

Erklärt mir die Begriffe Identifizierung, Authentifizierung und Authorisierung anhand einer Grenzkontrolle

- Identifikation $\rightarrow$ Ich sage wer ich bin

Identitätsüberprüfung

Wie überprüfe ich Identitäten und Berechtigungen?

Erklärt mir die Begriffe Identifizierung, Authentifizierung und Authorisierung anhand einer Grenzkontrolle

- Identifikation $\rightarrow$ Ich sage wer ich bin
- Authentifikation $\rightarrow$ Der Wächter kontrolliert wer ich bin

Identitätsüberprüfung

Wie überprüfe ich Identitäten und Berechtigungen?

Erklärt mir die Begriffe Identifizierung, Authentifizierung und Authorisierung anhand einer Grenzkontrolle

- Identifikation → Ich sage wer ich bin
- Authentifikation → Der Wächter kontrolliert wer ich bin
- Authorisierung → Der Wächter prüft was ich machen darf

Identitätsüberprüfung

Wie überprüfe ich Identitäten und Berechtigungen?

Erklärt mir die Begriffe Identifizierung, Authentifizierung und Authorisierung anhand einer Grenzkontrolle

- Identifikation → Ich sage wer ich bin
- Authentifikation → Der Wächter kontrolliert wer ich bin
- Authorisierung → Der Wächter prüft was ich machen darf

Richtige Reihenfolge

Authentifizierung muss immer vor der Authorisierung stattfinden! Identifikation ist ein optionaler Schritt. [a]

[a] `https://lithilion.at/blog/2024-12-identify-authenticate-authorise.html`

Implementierung (und Zerstörung) von Kryptographie

- Algorithmus ← hier setzt klassische Kryptoanalyse an
- Implementierung (Softwarebibliothek, Programm, Hardware, etc.)
- Benutzung
- Umweltfaktoren (Rechendauer, Stromverbrauch, Hitzeentwicklung, etc.)
- (Bruteforce)

Benötigtes Security Niveau

Das benötigte Security Niveau wird immer über das Vertraulichkeitslevel und die Lebensdauer der Information definiert!

Zusammenfassung

- Schutzziele der Information Security: CIA, SUE
- Kerkhoffsche Prinzip: Algorithmen sind Open-Source
- Identifikation, Authentifikation, Authorisierung
- Kryptoanalyse auf Algorithmus, Implementierung, Benutzer
- Security Niveau wird durch Vertraulichkeitslevel und Lebensdauer der Information definiert!

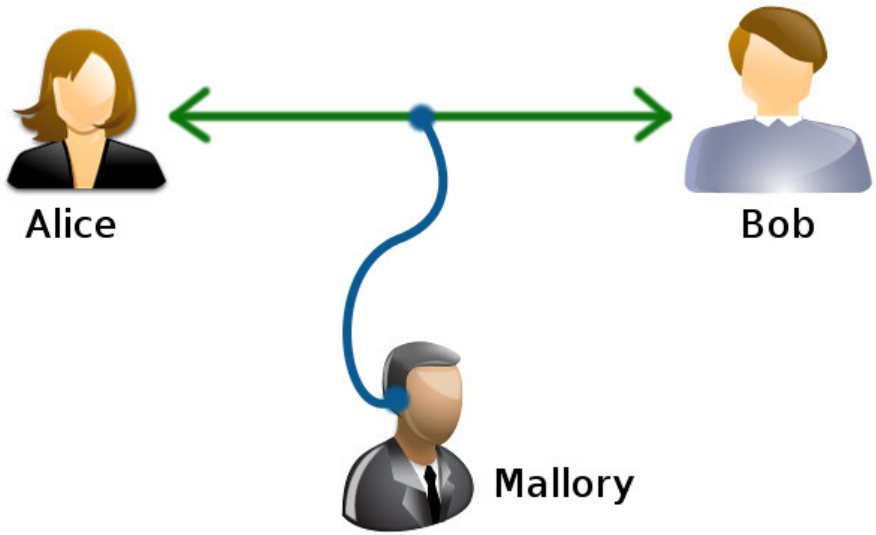
Symmetrische Kryptographie

Symmetrische Kryptographie

Ein Schlüssel für alles

2. Symmetrische Kryptographie
   - Erste Anfänge der Kryptographie
   - Moderne symmetrische Kryptographie
   - Block und Stromchiffren
   - Advanced Encryption Standard (AES)
   - One-Time-Pads (OTP)
   - Zusammenfassung

Rollenverteilung in der Kryptographie



Steganographie - Verstecke Informationen

- Militärische oder Regierungsgeheimnisse
- Umgehung von restriktiven Gesetzen, etc.
- DRM, etc.
- Schmuggel
- Privatsphäre

Steganographie - Beispiele

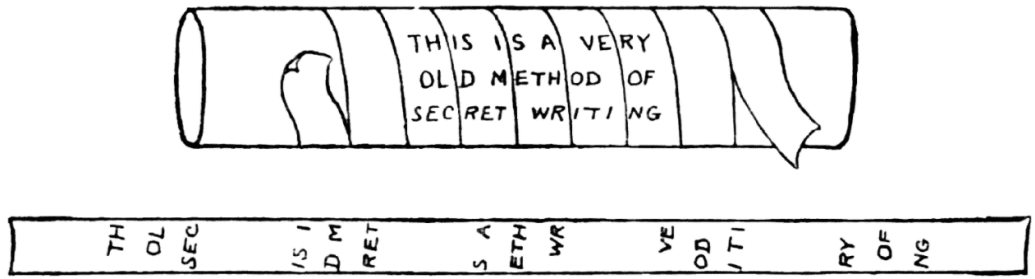
- Wachstafel
- Implementierung in Bildern
- „Schreiben“ mit Einschusslöchern in Ego-Shootern
- Oszilloskop
- True/Veracrypt - Plausible Deniability
- WoW Screenshot Watermarks:
  `https://www.reddit.com/r/Games/comments/zph9s/activision_blizzard_secretly_watermarking_world/`

Symmetrische Kryptographie

- Älteste Form der Kryptographie
- Lange Zeit einzige Form der Kryptographie
- Ein und derselbe Schlüssel für Ver- und Entschlüsseln

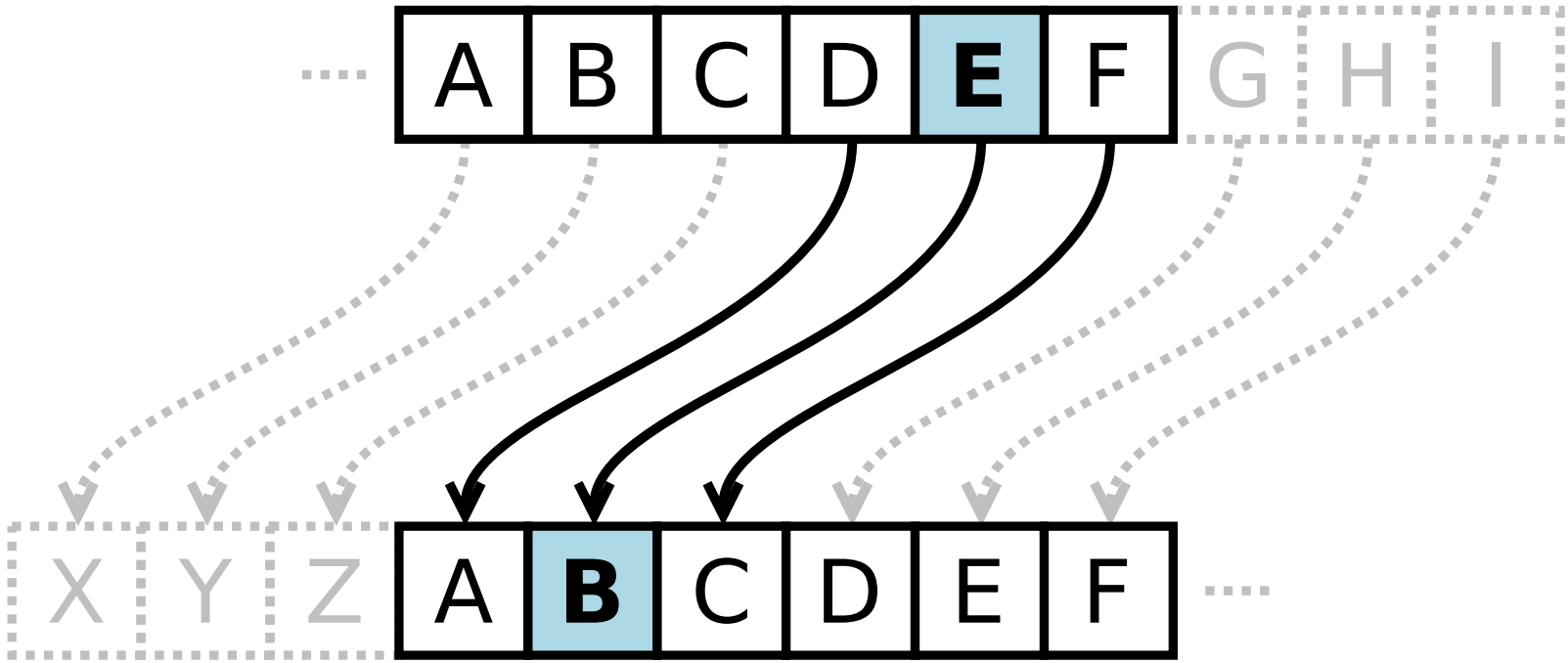
Spartanischer Stabschlüssel

- Stabdurchmesser ist der Schlüssel
- Einfache Art der Steganographie



Cäsar Cipher

- Substitutionscipher
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- FGHIJKLMNOPQRSTUVWXYZABCDE
- Schlüssel = 5
- CAESAR → HFKXFW



Cäsar Cipher - Übung

Namensverschlüsselung

Verschlüssle deinen Vor- und Nachname in Militärischer Schreibweise mit der Cäsar Cipher mit dem Schlüssel 6. Bei Umlauten und anderen Zeichen wird die Kreuzworträtselregel angewendet.

Cäsar Cipher - Übung

Namensverschlüsselung

Verschlüssle deinen Vor- und Nachname in Militärischer Schreibweise mit der Cäsar Cipher mit dem Schlüssel 6. Bei Umlauten und anderen Zeichen wird die Kreuzworträtselregel angewendet.

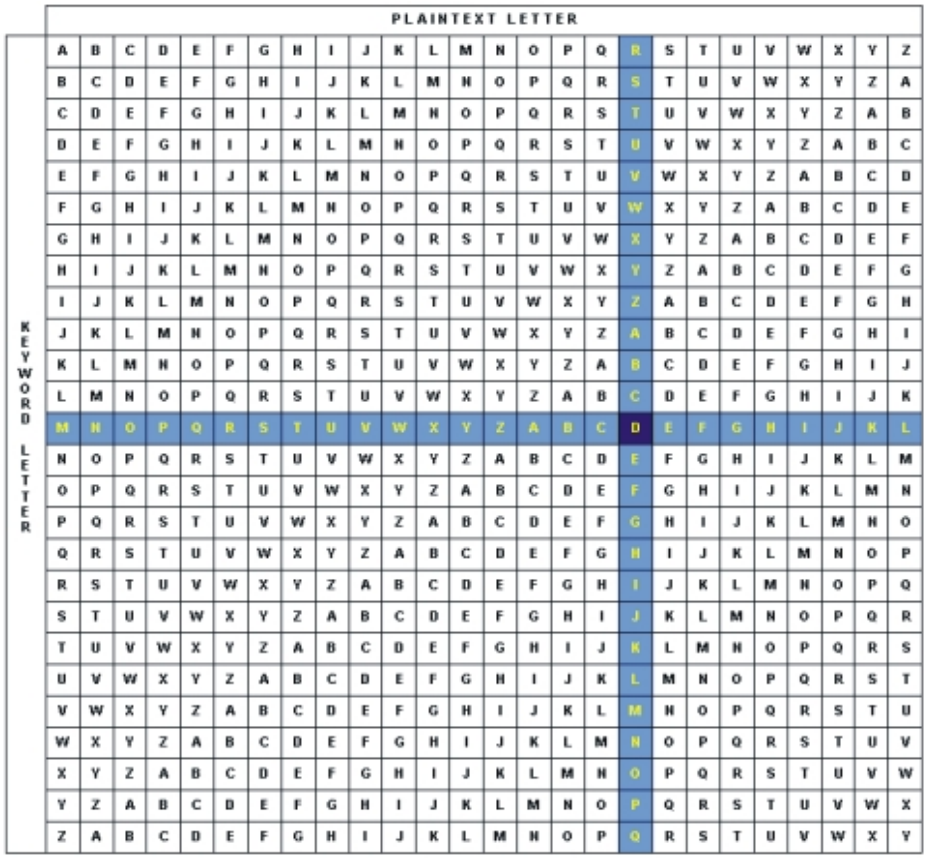
Schwachstelle Welche erste Schwachstelle kann entdeckt werden?

Encoding != Encryption

- Encoding: Zeichensubstitution anhand eines Algorithmus; bspw. Base64
- Encryption: Zeichensubstitution anhand eines Algorithmus UND eines Schlüssels; bspw. Cäsar

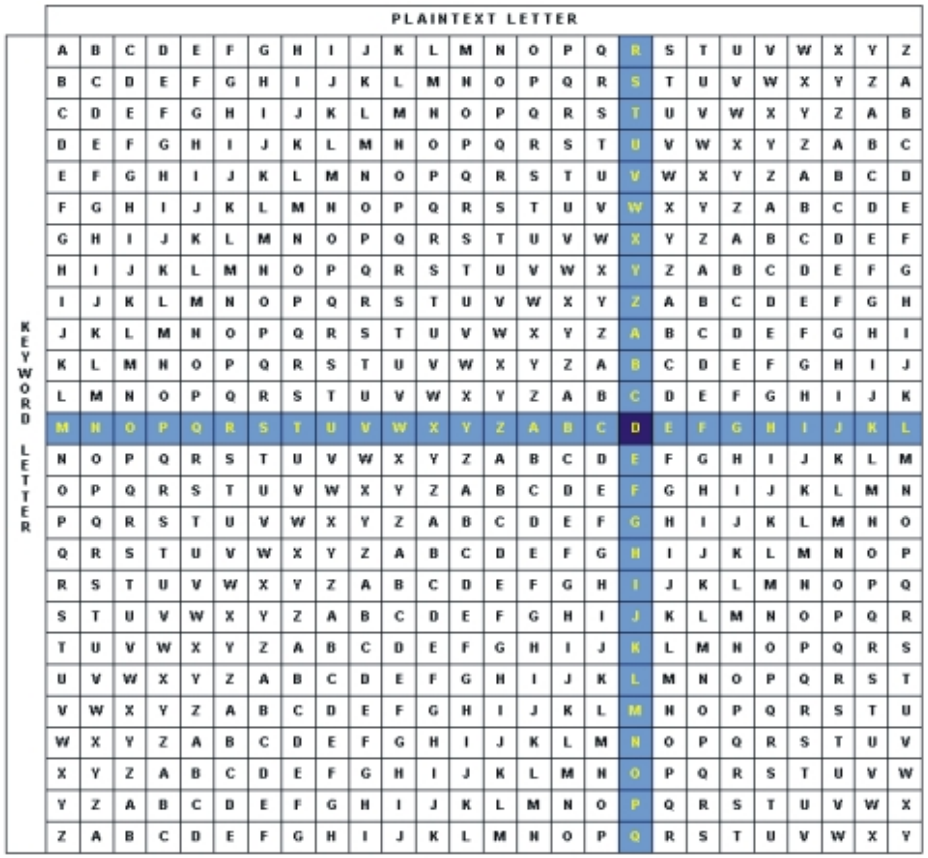
Vigenere Matrix

- Erfunden 1553, theoretisch gebrochen 1863, praktisch gebrochen 1920, großflächig in Verwendung bis 1940
- Verwendung im Feld durch Schweizer Armee bis 1970er
- Passwort: LIGHT
- Klartext: MORNING GLORY
- Ciphertext: XWXUBYO MSHCG



Vigenere Matrix

- Erfunden 1553, theoretisch gebrochen 1863, praktisch gebrochen 1920, großflächig in Verwendung bis 1940
- Verwendung im Feld durch Schweizer Armee bis 1970er
- Passwort: LIGHT
- Klartext: MORNING GLORY
- Ciphertext: XWXUBYO MSHCG



Lange Einsatzzeit

Warum wurde des Algorithmus so lange eingesetzt, obwohl er gebrochen war?

Vigenere Matrix - Übung

Verschlüssle und Entschlüssle

Verschlüssle und Entschlüssle deinen Nachnamen mit deinem Vornamen.

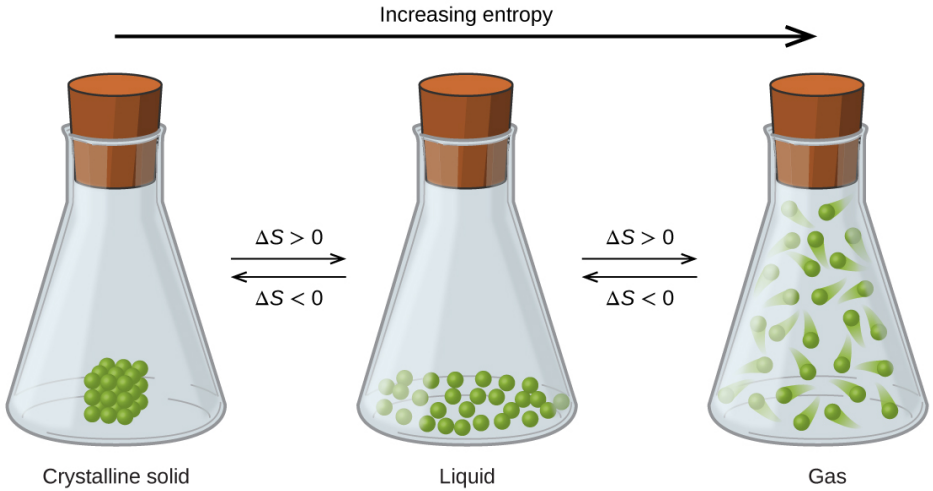
KEYWORD LETTER \ PLAINTEXT LETTER	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Mechanische und elektrische Kryptographie - Enigma

- Erste elektrische Chiffriermaschine
- Mit dem ersten „Computer“ gebrochen
  $\rightarrow$ Turing Bomb

Random-Number-Generator (RNG) & Entropie

- Große Entropie ist notwendig für starke Zufälligkeit und Kryptographie
- Beispiele für RNGs
  - Lava Lampe
  - Radioaktiver Zerfall
- Pseudo RNG
  - /dev/urandom
    - Arithmetischer Generator mit Initialisierungs Vektor
    - Entropie des OS (Diskauslastung, Netzwerk, etc.)



Enigma - Funktionsweise

Problem: Schlüsseltausch bzw. ein Schlüssel

Problem: Schlüsseltausch bzw. ein Schlüssel

- Wie übermittle ich Schlüssel über große Distanzen schnell und sicher?

Problem: Schlüsseltausch bzw. ein Schlüssel

- Wie übermittle ich Schlüssel über große Distanzen schnell und sicher?
- Wie erkenne und melde ich einen kompromittierten Schlüssel?

Problem: Schlüsseltausch bzw. ein Schlüssel

- Wie übermittle ich Schlüssel über große Distanzen schnell und sicher?
- Wie erkenne und melde ich einen kompromittierten Schlüssel?
- Wie stelle ich die Authentizität der Nachrichten sicher?

Problem: Schlüsseltausch bzw. ein Schlüssel

- Wie übermittle ich Schlüssel über große Distanzen schnell und sicher?
- Wie erkenne und melde ich einen kompromittierten Schlüssel?
- Wie stelle ich die Authentizität der Nachrichten sicher?
- Wie verhindere ich die mutwillige Weitergabe der Schlüssel?

Exkurs: Rechtliche Themen

- Militärische Geheimnisse
- Kalter Krieg
- Export und Import Bestimmungen von Wissen

Problematik

Exkurs: Rechtliche Themen

- Militärische Geheimnisse
- Kalter Krieg
- Export und Import Bestimmungen von Wissen

Problematik

Steht im Kontrast mit dem Kerckhoffschen Prinzip

Feistelnetzwerk

- Benannt nach Horst Feistel
- Großteil der heutigen symmetrischen Kryptographie basiert darauf
- Sammlung an Funktionen die iterativ in einer beliebigen Anzahl an Runden ausgeführt wird
- Verschlüssle Hälfte des Blocks und XOR mit anderer Hälfte des Blocks
- Einfache Implementierung in Hardware

DES - Data Encryption Standard

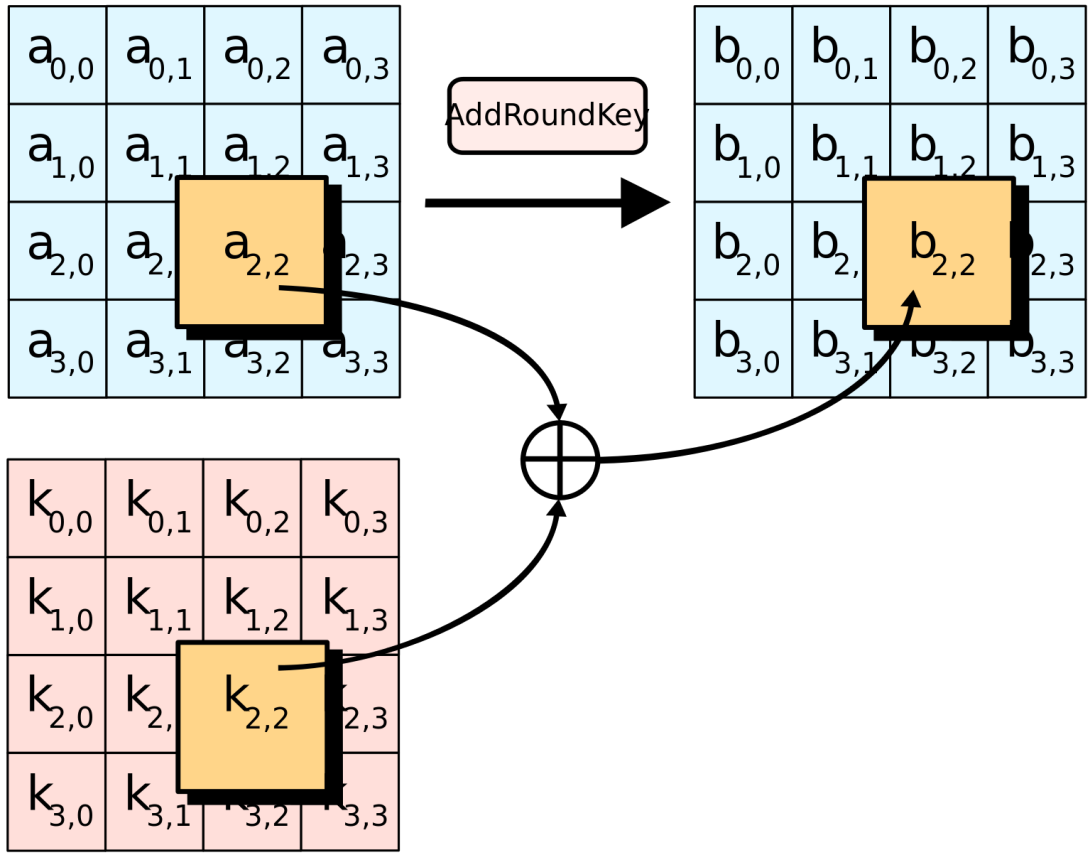
- Entwickelt durch IBM (Lucifer) und NSA zwischen 1970-1977
- Unterstützt nur 56-bit und hatte Backdoors
- 3DES; nur für Kompatibilität
- Moderne Smartphones knacken den Algorithmus in wenigen Sekunden
- Durch AES ersetzt worden

Auswahlverfahren

- Standardisierte, öffentliche Verfahren
- langlaufende Wettbewerbe
- AES: 1997-2000
- Post-Quantum-Cryptography: 2017-2024

Block Cipher

- Klartext und Schlüssel werden zu Blöcken transformiert
- Blöcke haben eine quadratische Größe (A x A bits)
- Benötigen oft einen Initialisierungsvektor (IV)

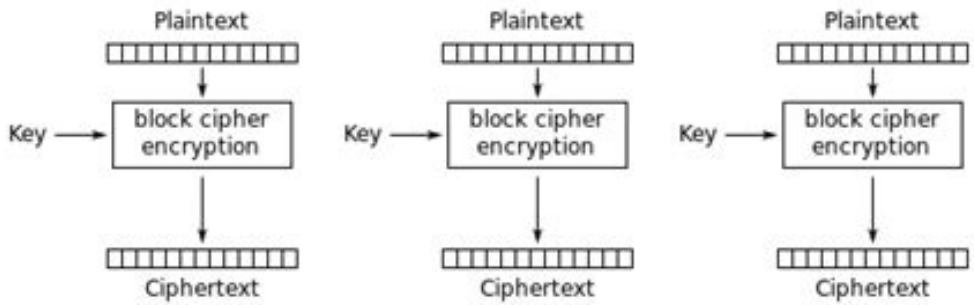


Zusammenbau Block Cipher

- Algorithmus: Wie wird ein Block behandelt?
- Modus: Wie werden die Blöcke verbunden?

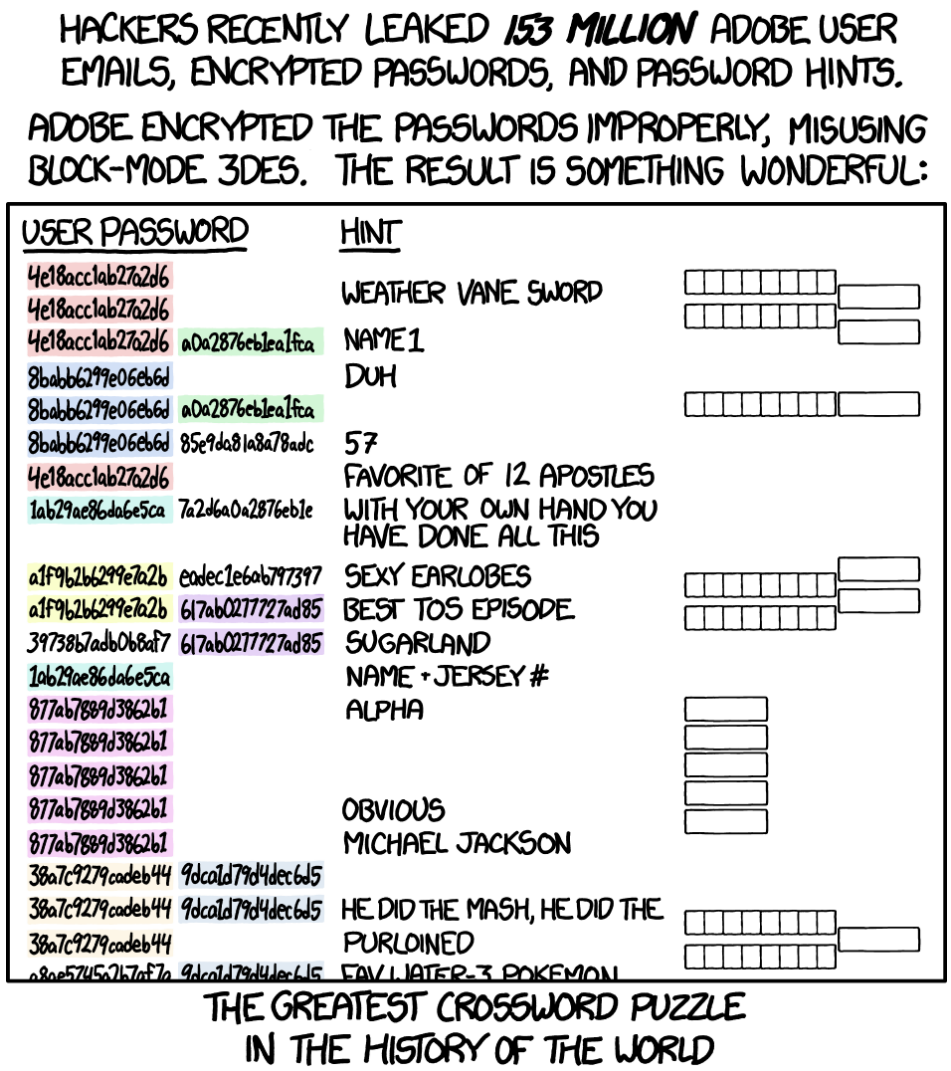
ECB Modus

- Ältester Modus
- Einfach
- Unsicher



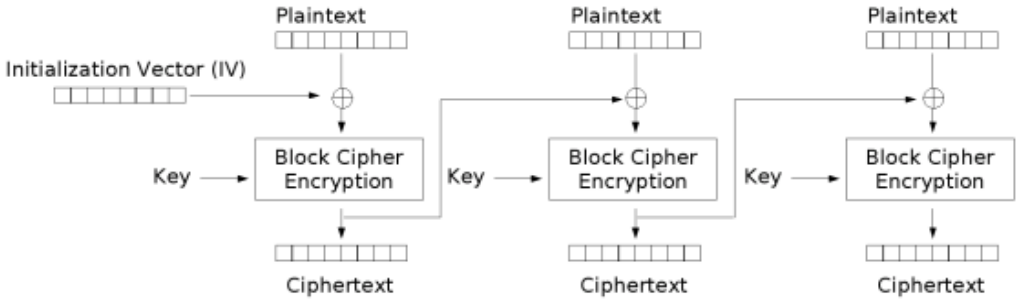
Electronic Codebook (ECB) mode encryption

Problem mit ECB



CBC Modus

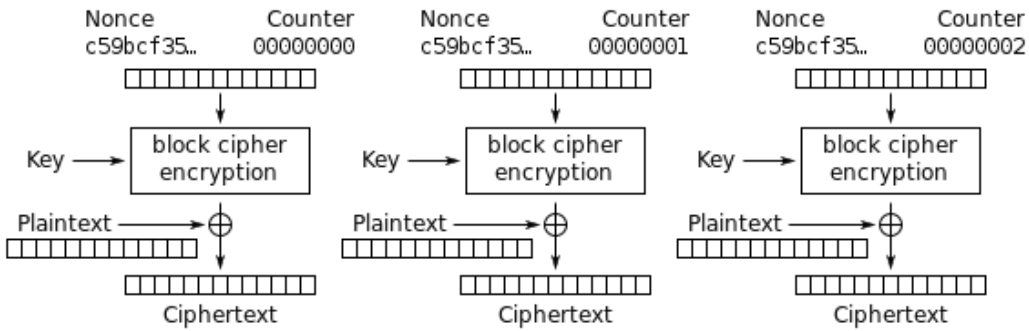
- Sicherer als ECB
- Langsam, „entschlüssle immer alles“
- Vulnerabel zum Padding Oracle Angriff



Cipher Block Chaining (CBC) mode encryption

CTR Modus

- Sicher, schnell
- Verschlüssle einen Zähler
- XOR den Klartext

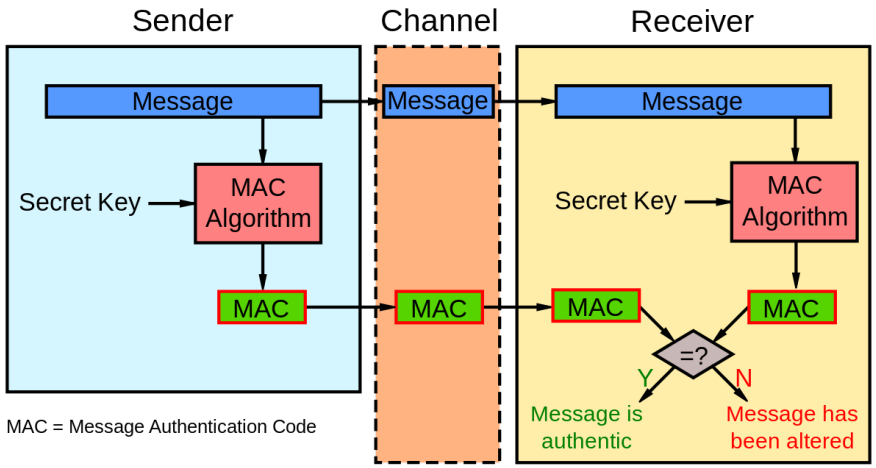


Counter (CTR) mode encryption

GCM Modus

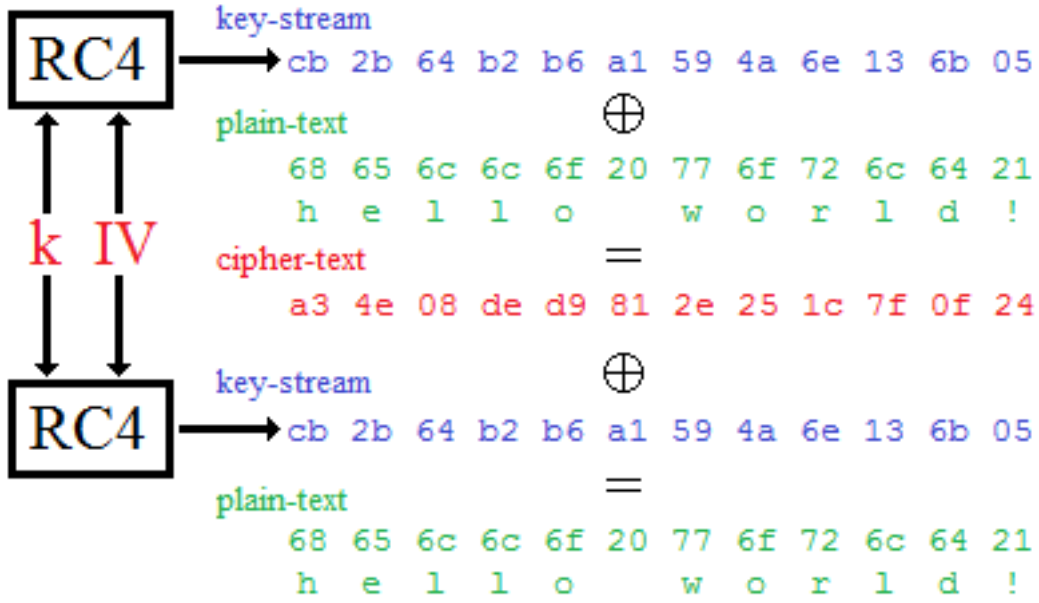
- Modern
- Verschlüssle, dann mach einen MAC
- Erweiterung des CTR
- Authentifiziere mit einem Galois Feld
- AES-GCM ist Teil von IPsec, SSH, TLS 1.2 und 1.3

MAC - Message Authentication Code



Stream Cipher

- Single-Use selbst produzierter Schlüsselstrom
- RC4 ist alt und gebrochen, aber (leider) noch häufig im Einsatz
- Salsa20 ist momentan der Standard (XOR Nonce, Zähler, Schlüssel)
- Wird benutzt in GSM, TLS, Torrenting, etc.

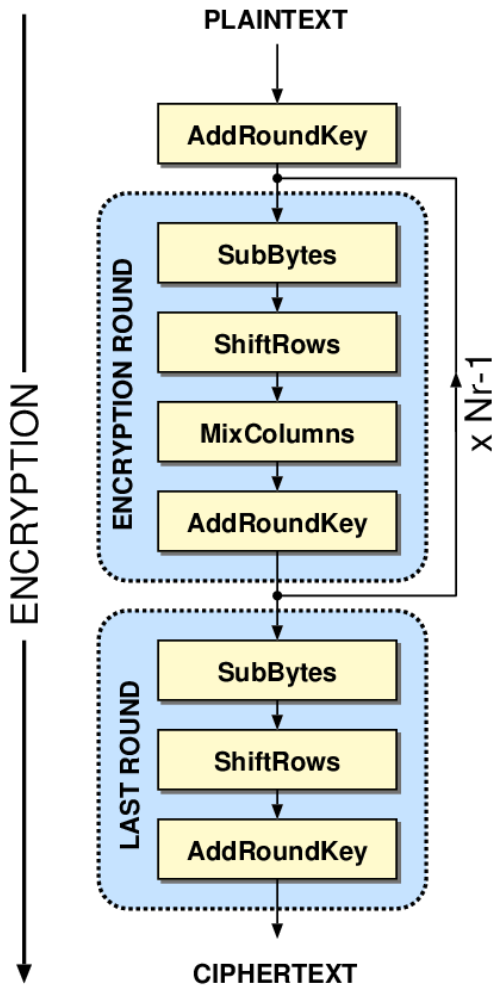


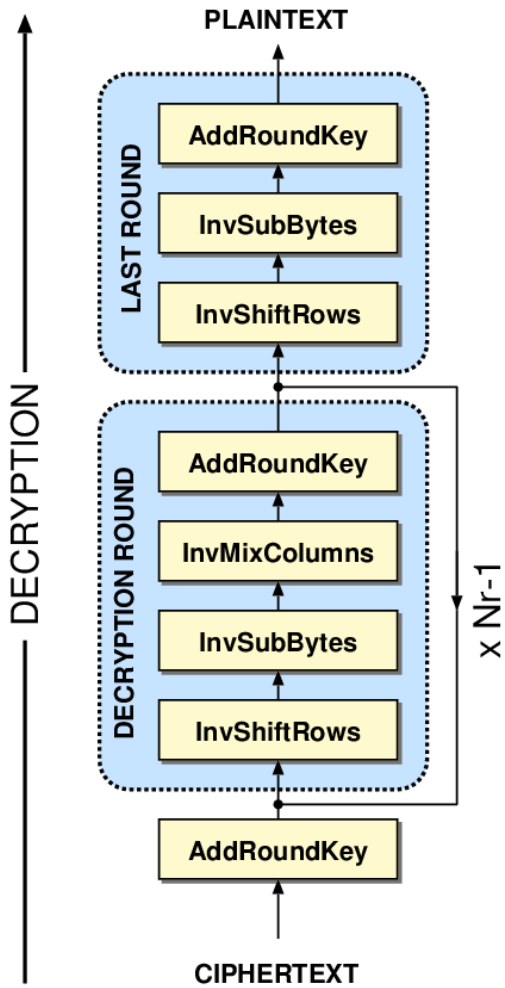
AES - Advanced Encryption Standard

- Standartisiert durch NIST im Jahr 2000
- **Rijndael**, Serpent, Twofish, RC6, MARS
- Schnell und sicher
- Oft implementiert in Hardware
- Bis heute keine bekannten, erfolgreichen Angriffe
- Laut Snowden auch bei der NSA nichts bekanntes (2013)
- Confusion: Obskure Zusammenhänge zwischen Klar und Ciphertext
- Diffusion: Verteilung des Klartexts über große Bereiche des Ciphertexts

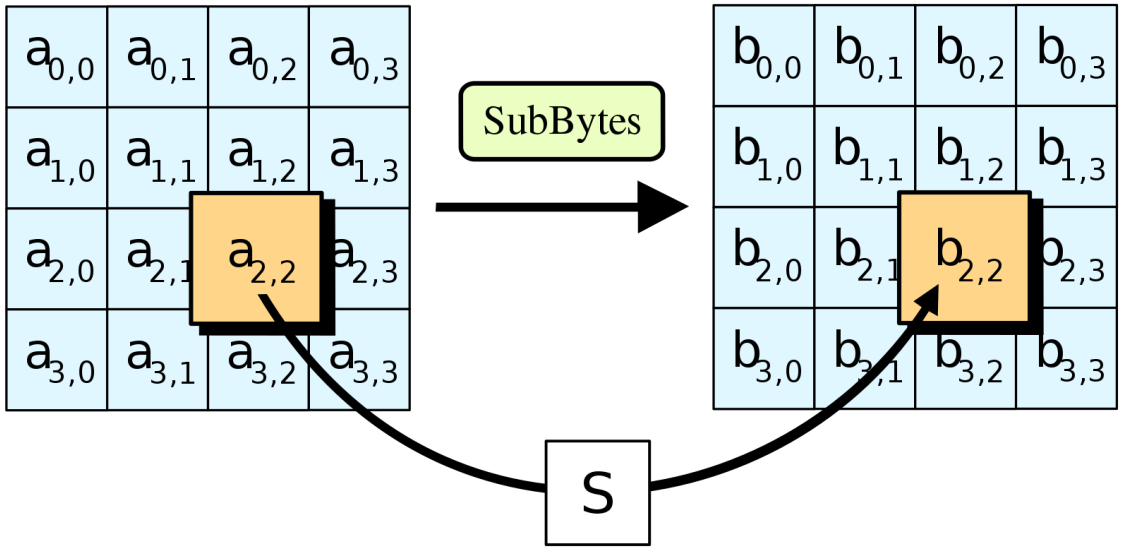
AES - Algorithmus

- Bekannteste, meist verbreitete Block Cipher
- 10 Runden für 128-bit Schlüssel
- 12 Runden für 192-bit Schlüssel
- 14 Runden für 256-bit Schlüssel
- SubBytes: Confusion
- ShiftRows, MixColumns: Diffusion





AES - SubBytes

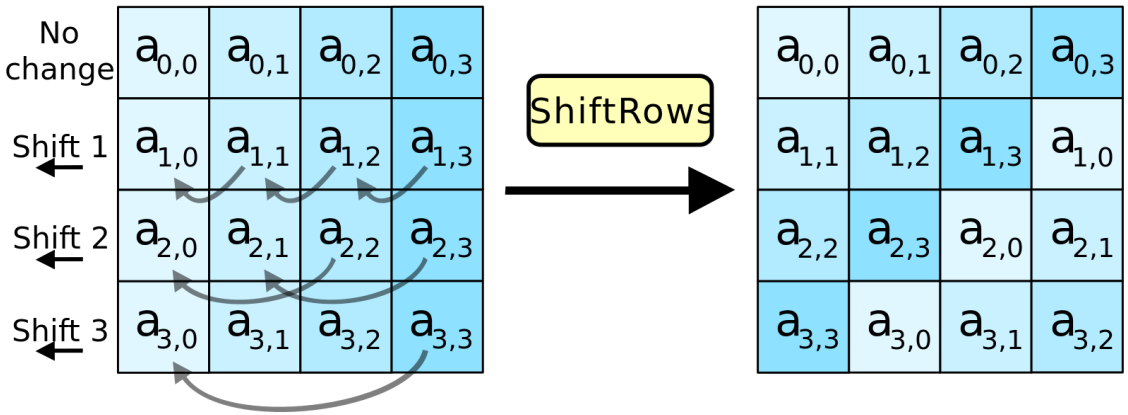


S - Box

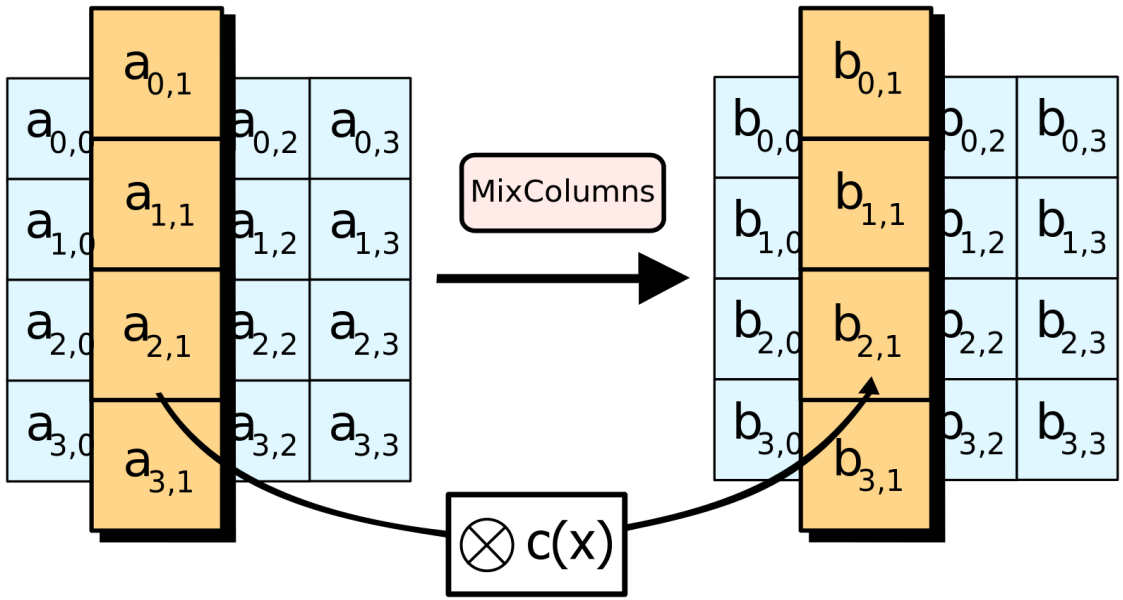
(Errechnete) Box zum Substituieren von Klartextbits $\rightarrow$Konfusion.
Anforderungen

- Vollständigkeit — Jedes Ausgangsbit ist abhängig vom Eingangsbit.
- Lawine — Änderung an einem Eingangsbit ändert zumindest die Hälfte der Ausgangsbits.
- Nichtlinearität — Ausgangsbits sind nicht linear abhängig von Eingangsbits.
- Korrelationsimmunität — Alle Ein- und Ausgangsbits müssen bekannt sein um das Gegenstück zu finden.

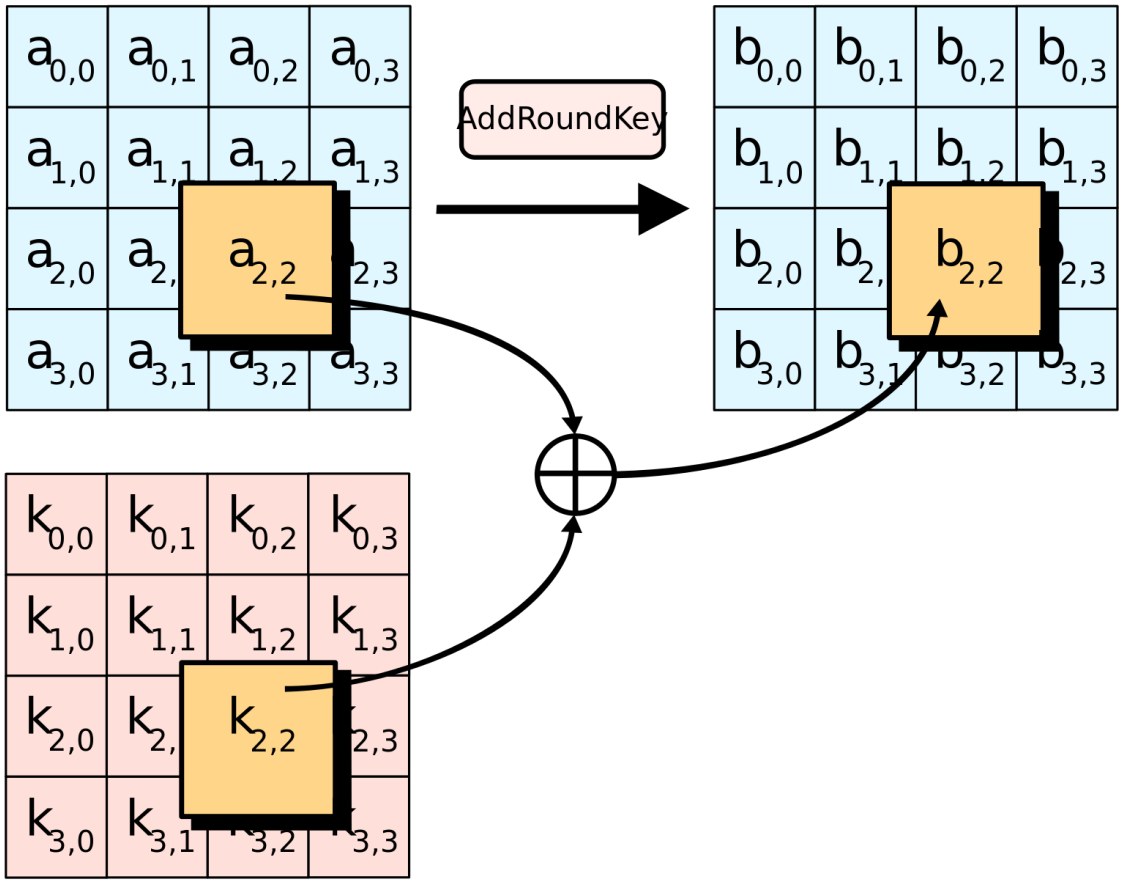
AES - ShiftRows



AES - MixColumns

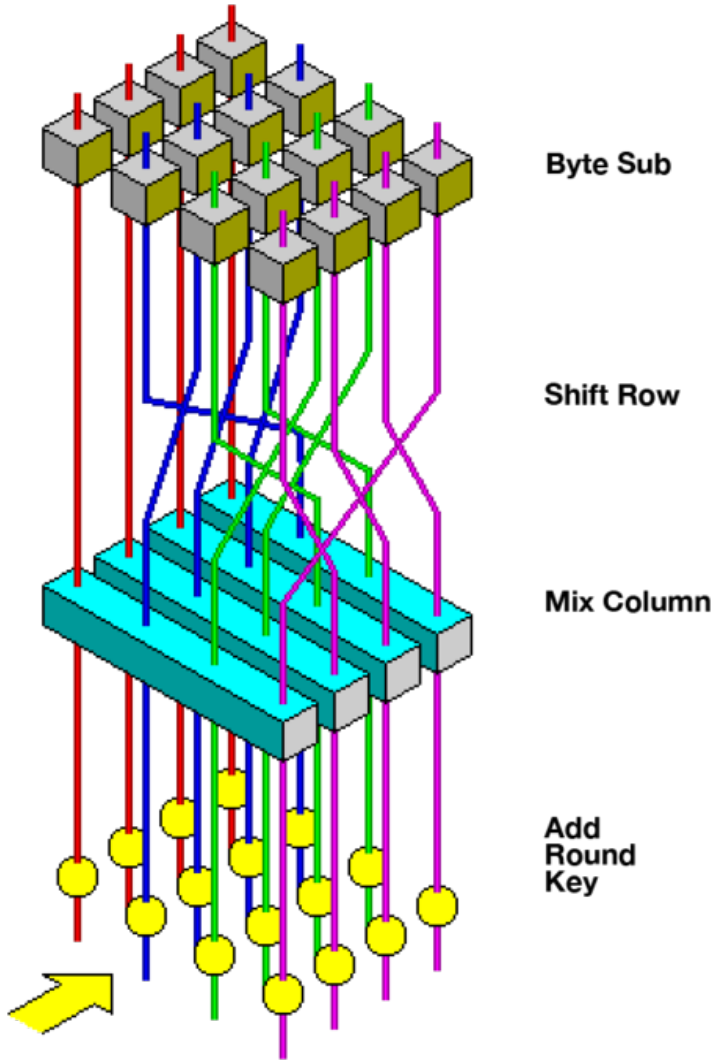


AES - AddRoundKey



AES - Algorithmus

- Bekannteste, meist verbreitete Block Cipher
- 10 Runden für 128-bit Schlüssel
- 12 Runden für 192-bit Schlüssel
- 14 Runden für 256-bit Schlüssel
- SubBytes: Confusion
- ShiftRows, MixColumns: Diffusion



AES - Übung

Blockgröße

Warum werden immer 4x4 große Blöcke angezeigt?

AES - Übung

Blockgröße

Warum werden immer 4x4 große Blöcke angezeigt?

AES berechnen

Wir berechnen eine Runde AES eines Blocks mit einem ausgewählten Text und Schlüssel. Angabe: `https://git.nwt.fhstp.ac.at/lblackner/prc/-/jobs/artifacts/master/file/out/aes.pdf?job=make`

OTP - One Time Pad

- Unknackbare Kryptographie
- Single-Use PSK
- XOR Klartext und Schlüssel
- Schlüssel muss die Länge des Klartexts haben
- Äußerst selten eingesetzt (Nachrichtendienste, Agentenkommunikation, etc.)

OTP - One Time Pad

- Unknackbare Kryptographie
- Single-Use PSK
- XOR Klartext und Schlüssel
- Schlüssel muss die Länge des Klartexts haben
- Äußerst selten eingesetzt (Nachrichtendienste, Agentenkommunikation, etc.)

Einsatzhäufigkeit

Warum wird der Algorithmus so selten eingesetzt? Stichwort SUE

Zusammenfassung Symmetrische Kryptographie

- Ein Schlüssel für alles
- Schlüsseltauschproblem
- Volles Vertrauen zu anderer Stelle
- Post-Quanten sicher
- Vermeide deterministische Ciphertexte
- Block und Stream Cipher
- Algorithmen und Modi

Asymmetrische Kryptographie

Asymmetrische Kryptographie

Mehrere Schlüssel für mehrere Anwendungen

3. Asymmetrische Kryptographie
   - Grundlagen und Geschichte
   - Diffie-Hellman (DH)
   - Diskreter-Logarithmus-Problem (DLP)
   - Rivest-Shamir-Adelman (RSA)
   - Digitale Zertifikate
   - Vergleich von (A)symmetrischer Kryptographie
   - Post-Quantum-Cryptography (PQC)
   - Zusammenfassung

Problem: Schlüsseltausch bzw. ein Schlüssel

- Wie übermittle ich Schlüssel über große Distanzen schnell und sicher?
- Wie erkenne und melde ich einen kompromittierten Schlüssel?
- Wie stelle ich die Authentizität der Nachrichten sicher?
- Wie verhindere ich die mutwillige Weitergabe der Schlüssel?

Grundlegendes

- Zwei Schlüssel
- Public Key für die Öffentlichkeit
- Private Key bleibt geheim

Grundlegendes

- Zwei Schlüssel
- Public Key für die Öffentlichkeit
- Private Key bleibt geheim
- Unterschiedliche Schlüssel für Verschlüsselung und Entschlüsselung
- Löst das Schlüsseltausch Problem

Perfect Forward Secrecy

- Tausche die Schlüssel regelmäßig aus
- Wenn ein Schlüssel kompromittiert wird, betrifft das nur diesen und neuere Schlüssel, NICHT aber das Archiv!

Modulo Rechnen

- „Rest-Rechnen“
- $10/5 = 2$
- $10\%5 = 0$

Modulo Rechnen

- „Rest-Rechnen“
- $10/5 = 2$
- $10\%5 = 0$
- $7/4 = 1,75$
- $7\%4 = 3$

Modulo Rechnen

- „Rest-Rechnen“
- $10/5 = 2$
- $10\%5 = 0$
- $7/4 = 1,75$
- $7\%4 = 3$

Modulo Rechnen

Modulo Rechnen bedeuted eine Division, aber das gesuchte Ergebnis ist der Rest der Division. Das Ergebnis einer Modulorechnung ist IMMER eine natürliche Zahl.

Übung: Modulo Rechnen

- $22\%4 =$

Übung: Modulo Rechnen

- $22\%4 =$
- $4556 mod 43 \equiv$

Übung: Modulo Rechnen

- $22\%4 =$
- $4556 mod 43 \equiv$
- $7553^2 mod 17 = 57047809 mod 17 \equiv$

Übung: Modulo Rechnen

- $22\%4 =$
- $4556 mod 43 \equiv$
- $7553^2 mod 17 = 57047809 mod 17 \equiv$
- $7553^6 mod 17 \equiv$

Übung: Modulo Rechnen

- $22\%4 =$
- $4556 mod 43 \equiv$
- $7553^2 mod 17 = 57047809 mod 17 \equiv$
- $7553^6 mod 17 \equiv$

Rechne

Schreibe ein Skript um $7553^{10} mod 17$ schnell und ressourcenschonend rechnen zu können. Funktioniert es auch mit $43^{20} mod 50$?

Primfaktoren und Zerlegung

- Primzahl: Nur durch 1 und sich selbst teilbar.
- Jede natürliche Zahl kann in Primzahlen faktoriert werden. Bsp.: $6 = 2 * 3$, $18 = 2 * 3 * 3$ und $19 = 19$

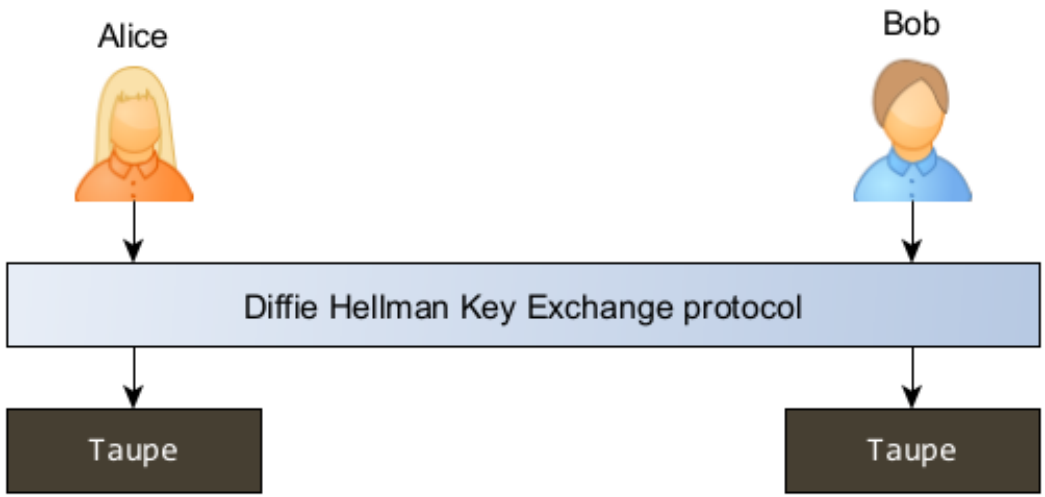
Primfaktoren und Zerlegung

- Primzahl: Nur durch 1 und sich selbst teilbar.
- Jede natürliche Zahl kann in Primzahlen faktoriert werden. Bsp.: $6 = 2 * 3$, $18 = 2 * 3 * 3$ und $19 = 19$
- Kein effizientes Verfahren zur Primfaktorzerlegung bekannt.

Diffie-Hellman Schlüsselaustausch

- Erzeuge geheime symmetrische Schlüssel über einen öffentlichen, unsicheren Kanal aus.
- Erfunden 1976
- Whitfield Diffie & Martin Hellman

DH - Farbkübelanalogie



Wir wollen mit einem Algorithmus einen gemeinsamen, geheimen Schlüssel erstellen.

DH - Farbkübelanalogie

Wir wählen ein gemeinsame Farbe.

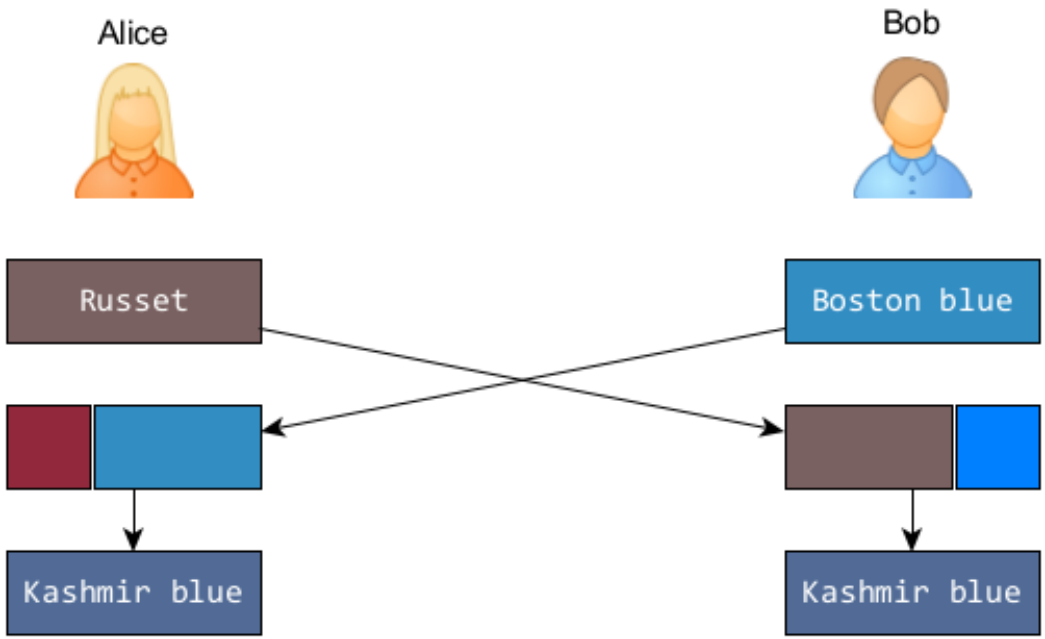
DH - Farbkübelanalogie

Jeder wählt eine geheime Farbe für sich selbst.

DH - Farbkübelanalogie

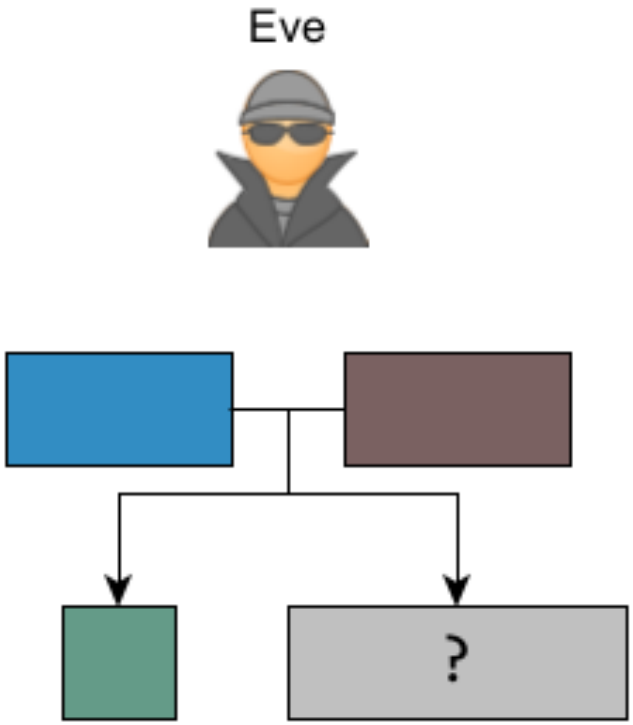
Wir vermischen die geheime Farbe mit der gemeinsamen Farbe.

DH - Farbkübelanalogie



Wir bekommen das Ergebnis der jeweils anderen Mischung und mischen unsere eigene geheime Farbe in die erhaltene Mischung. Das Ergebnis auf beiden Seiten ist ident.

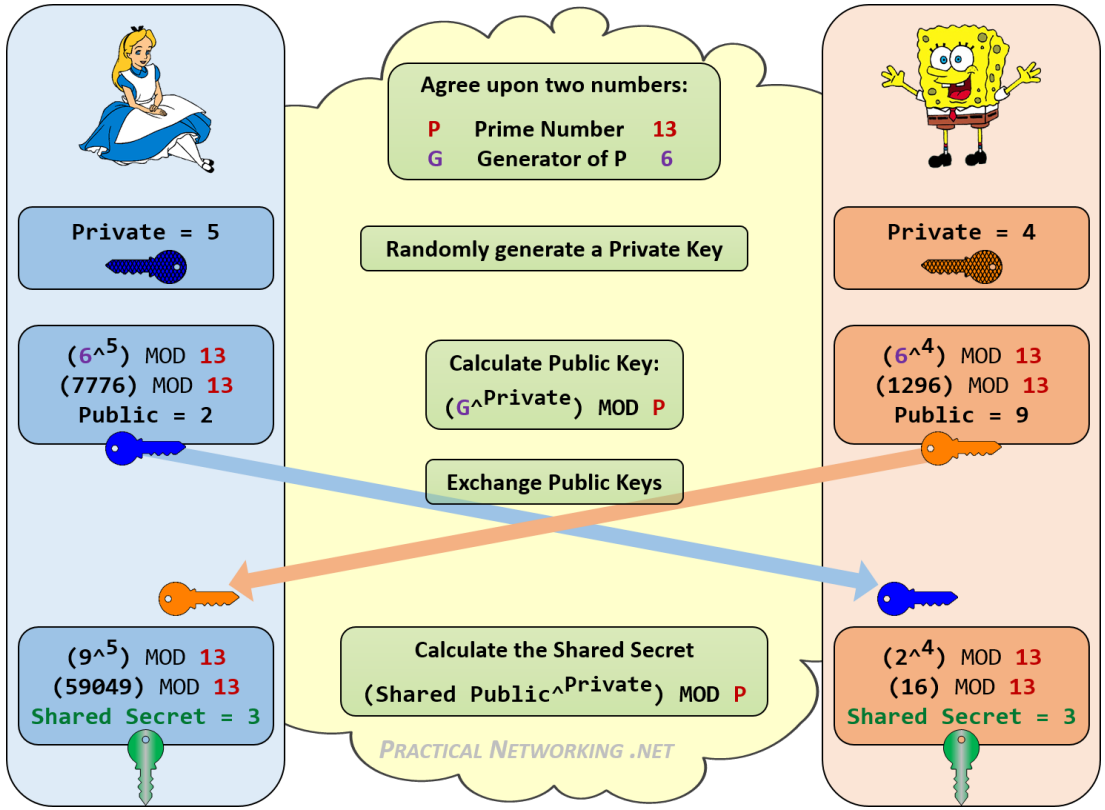
DH - Farbkübelanalogie



Der Angreifer erhält die Zwischenmischung und weiß dass ein Bestandteil die gemeinsame Farbe ist. Welche beiden Farben hier noch inbegriffen sind, ist sehr schwer herauszufinden.

Diffie-Hellman berechnen

1. $a = 5$
2. $b = 4$
1. $A = G^a \mod P = 2$
2. $B = G^b \mod P = 9$
1. $A^b \mod P = (G^a)^b \mod P = G^{ab} \mod P = 3$
2. $B^a \mod P = (G^b)^a \mod P = G^{ab} \mod P = 3$



Diskreter Logarithmus Problem (DLP)

- $g^x mod p \equiv h$
- g, p, h sind bekannt
- kein Weg bekannt um x mit traditionellen Mitteln zu finden

Diskreter Logarithmus Problem (DLP)

- $g^x mod p \equiv h$
- g, p, h sind bekannt
- kein Weg bekannt um x mit traditionellen Mitteln zu finden
- x ist der private Schlüssel

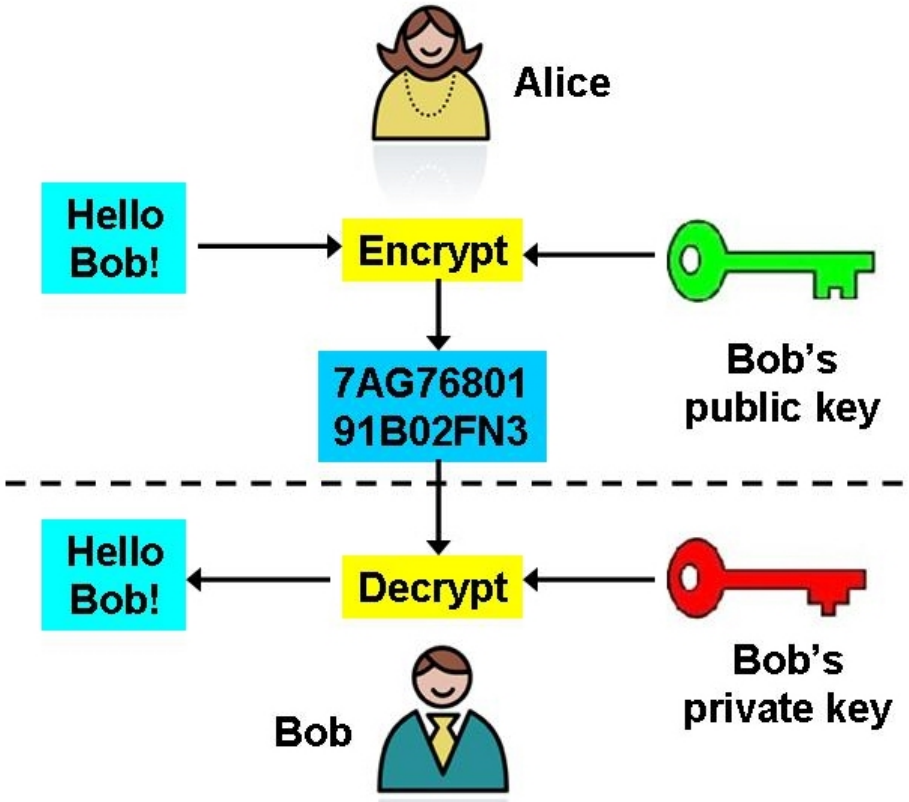
Diskreter Logarithmus Problem (DLP)

- $g^x mod p \equiv h$
- g, p, h sind bekannt
- kein Weg bekannt um x mit traditionellen Mitteln zu finden
- x ist der private Schlüssel
- Achtung! Quanten Computer kann das. $\rightarrow$Shors Algorithmus

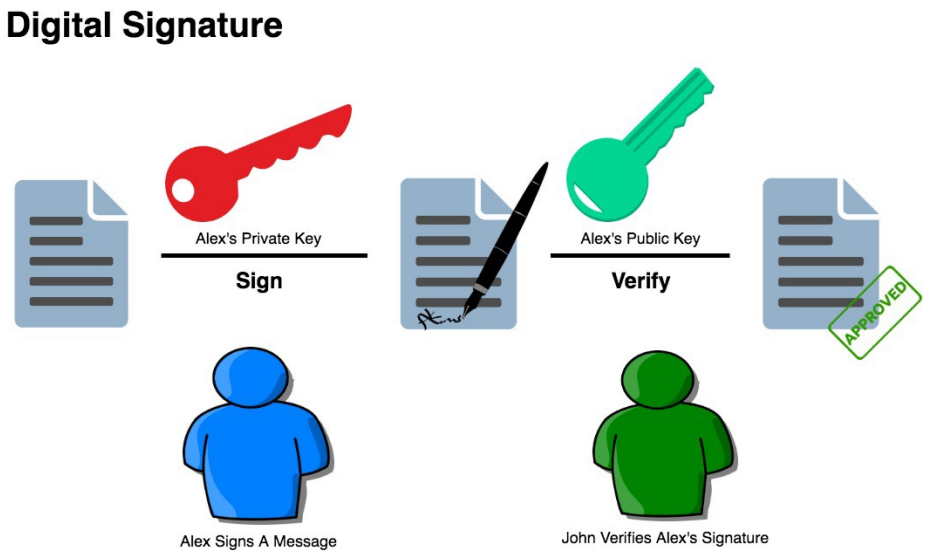
RSA - Rivest Shamir Adleman

- Bekanntester Asymmetrischer Algorithmus
- Veröffentlicht 1977
- Bereits 1973 vom GCHQ gefunden, erst 1997 deklassifiziert
- Schlüsselgröße 2048-4096 Bit (vgl. AES mit 128 Bit)
- Basiert auf dem DLP, daher nicht Post-Quanten tauglich
- Recht langsam
- Alles wird als natürliche Zahl angesehen
- Schlüssel wird berechnet, nicht gewählt!

Public Key Kryptographie - Verschlüsseln



Public Key Kryptographie - Signieren



RSA - Schlüssel berechnen

- P =Zufällige Primzahl $\rightarrow$Geheim
- Q =Zufällige Primzahl $\rightarrow$Geheim
- $N = P * Q$ $\rightarrow$Öffentlich
- $\phi(N) = (P-1) * (Q-1)$ $\rightarrow$Geheim
- E =Zufällige Primzahl kleiner als $\phi(N)$ $\rightarrow$Öffentlicher Schlüssel
- D =Inverse Modulo von E in $\phi(N)$ $\rightarrow$Geheimer Schlüssel

RSA - Verschlüsseln & Entschlüsseln

- $x^E mod N =$ Ciphertext
- $y^D mod N =$ Klartext

Verwendung des Schlüsselpaares

- Privater (geheimer) Schlüssel — Entschlüsseln, Signieren
- Öffentlicher Schlüssel — Verschlüsseln, Überprüfen

RSA - Übung

RSA berechnen

Wir berechnen eine Schlüssel für RSA und verschlüsseln und entschlüsseln einen ausgewählten Text. Angabe:
`https://git.nwt.fhstp.ac.at/lblackner/prc/-/jobs/artifacts/master/file/out/rsa.pdf?job=make`

RSA - Übung

RSA berechnen

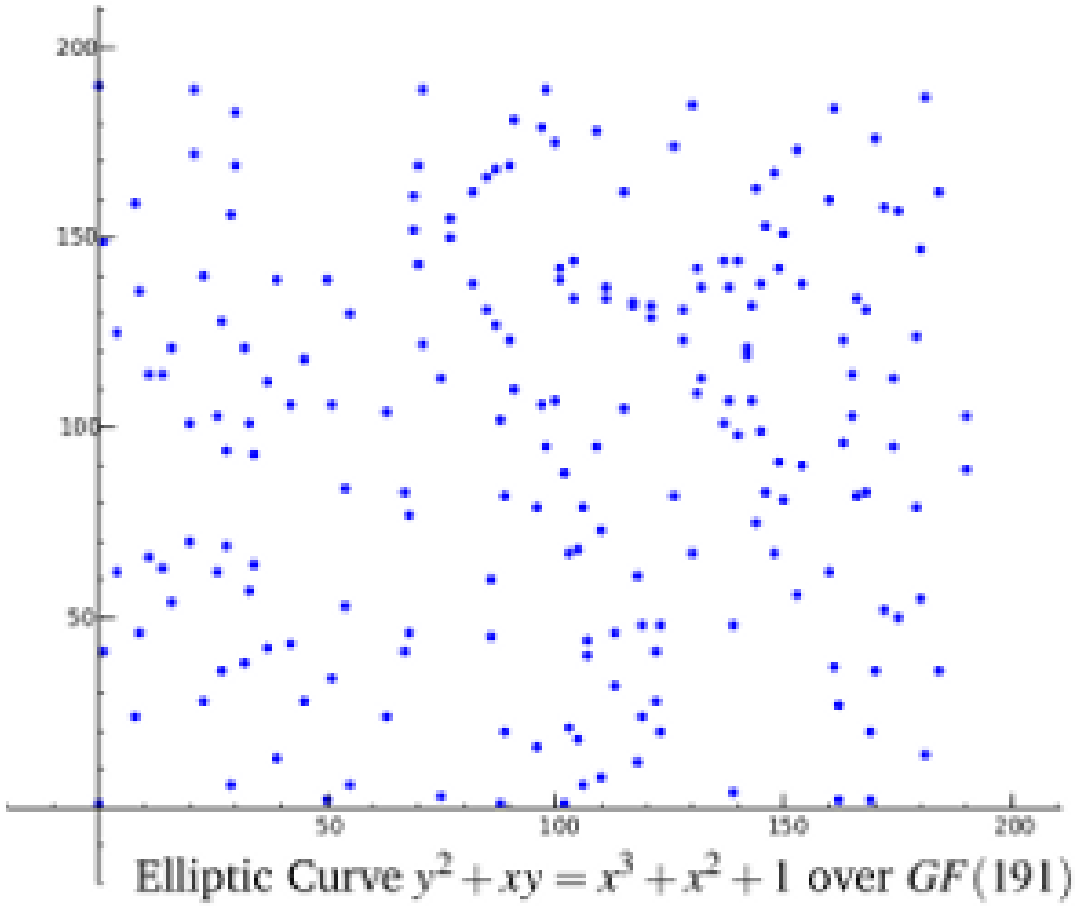
Wir berechnen eine Schlüssel für RSA und verschlüsseln und entschlüsseln einen ausgewählten Text. Angabe:
`https://git.nwt.fhstp.ac.at/lblackner/prc/-/jobs/artifacts/master/file/out/rsa.pdf?job=make`

Geschwindigkeit

Mit welcher Cipher wird der Computer schneller und resourcenärmer einen Ciphertext berechnen können? RSA oder AES? Warum?

EC - Elliptische Kurven

- Bessere Security
- Bessere Effizienz
  - Schneller
  - Geringere Schlüssellängen



Übung: Berechnungszeiten

Übung

Schreibe ein Skript um mittels openssl Schlüssel für folgende Algorithmen in der Standardstärke zu berechnen und miss die vergangene Zeit pro Algorithmus im Millisekundenbereich: RSA-2048, Curve25519, AES-128. Was kann man erkennen?

Digitale Zertifikate

Ein digitales Zertifikat beinhaltet:

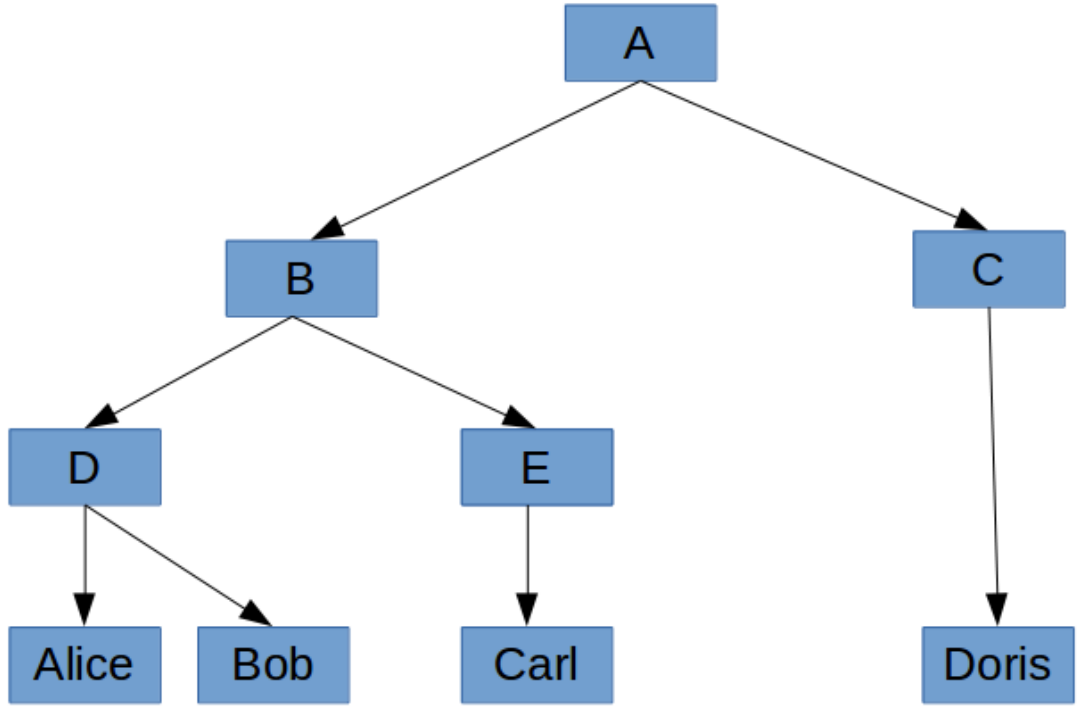
- Schlüssel(paar)
- Metadaten des Besitzers
  - Name
  - Email Addresse
  - URL
  - etc.

Verwaltung und Verteilung von Zertifikaten

- PKI - Public Key Infrastructure
- WoT - Web of Trust

PKI - Public Key Infrastructure

- eIDAS [a]
- SMIME
- Add Root Certificate to PKI: [b]
- Zentral verwaltet, dadurch Auslagerung des Vertrauens an zentrale Stelle (kann auch extern sein)

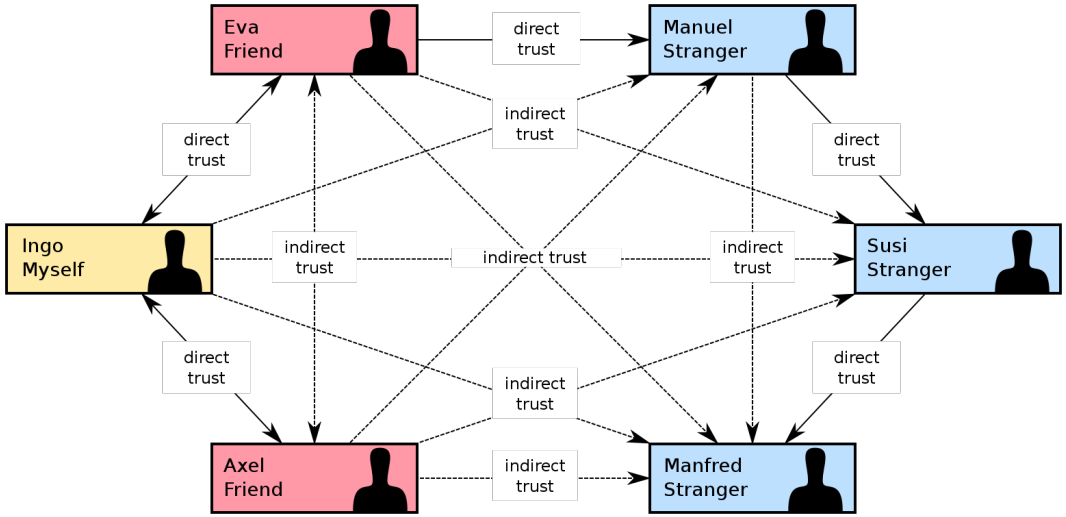


[a] https://eidas.ec.europa.eu/efda/browse/notification/eid-chapter-contacts

[b] https://bugzilla.mozilla.org/show_bug.cgi?id=647959

WoT - Web of Trust

- Selbst verwaltet, wesentlich höherer Verwaltungsaufwand. Unterschiedliche Vertrauensstände.
- Cryptoparties
- PGP



Umgang Schlüsselpaar - Übung

Umgang mit dem Schlüsselpaar

Wie gehen Sie mit den folgenden Situationen um?

Umgang Schlüsselpaar - Übung

Umgang mit dem Schlüsselpaar

Wie gehen Sie mit den folgenden Situationen um?

- Es muss ein Text verschlüsselt werden. Welcher Schlüssel wird verwendet?

Umgang Schlüsselpaar - Übung

Umgang mit dem Schlüsselpaar

Wie gehen Sie mit den folgenden Situationen um?

- Es muss ein Text verschlüsselt werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text signiert werden. Welcher Schlüssel wird verwendet?

Umgang Schlüsselpaar - Übung

Umgang mit dem Schlüsselpaar

Wie gehen Sie mit den folgenden Situationen um?

- Es muss ein Text verschlüsselt werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text signiert werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text verschlüsselt und signiert werden. Welcher Schlüssel wird verwendet?

Umgang Schlüsselpaar - Übung

Umgang mit dem Schlüsselpaar

Wie gehen Sie mit den folgenden Situationen um?

- Es muss ein Text verschlüsselt werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text signiert werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text verschlüsselt und signiert werden. Welcher Schlüssel wird verwendet?
- Sie erhalten ein digitales Zertifikat von jemand anderem. Was tun Sie?

Umgang Schlüsselpaar - Übung

Umgang mit dem Schlüsselpaar

Wie gehen Sie mit den folgenden Situationen um?

- Es muss ein Text verschlüsselt werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text signiert werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text verschlüsselt und signiert werden. Welcher Schlüssel wird verwendet?
- Sie erhalten ein digitales Zertifikat von jemand anderem. Was tun Sie?
- Dieses Zertifikat enthält dessen private Schlüssel. Was tun Sie?

Umgang Schlüsselpaar - Übung

Umgang mit dem Schlüsselpaar

Wie gehen Sie mit den folgenden Situationen um?

- Es muss ein Text verschlüsselt werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text signiert werden. Welcher Schlüssel wird verwendet?
- Es muss ein Text verschlüsselt und signiert werden. Welcher Schlüssel wird verwendet?
- Sie erhalten ein digitales Zertifikat von jemand anderem. Was tun Sie?
- Dieses Zertifikat enthält dessen private Schlüssel. Was tun Sie?
- Sie bekommen für die Implementierung und Konfiguration eines Dienstes ein Zertifikat inkl. privater Schlüssel zugewiesen. Was tun Sie?

Vergleich von (A)symmetrischer Kryptographie

- Moderne symmetrische Kryptographie ist Bitverschieben und XORing
- Traditionelle asymmetrische Kryptographie setzt stark auf Primzahlen und Modulorechnen (PQC funktioniert anders)

Apokalypse der Public-Key-Kryptographie

- Theoretischer Angriff durch Shors Algorithmus auf DLP-basierte Kryptographie
- Benötigt Quantencomputer zur Durchführung
- Quantencomputer ist bereits verfügbar, Rechenleistung ist noch begrenzt
- 2019: IBM 20-Qubits
- 2022: IBM: 433-Qubits[1]
- Problematisch bei langer Lebensdauer der Information!

[1] https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generatio

Post Quantum Cryptography

- NIST Standards
  - ML-KEM (Kyber) - Key Encapsulation
  - ML-DSA (Dilithium) - Digital Signature
  - SLH-DSA (Sphincs+) - Digital Signature
  - (FN-DSA - Falcon) - Digital Signature
  - FIPS 203,204,205
- Bereits erste Implementierungen in OpenSSH

Zusammenfassung Asymmetrische Kryptographie

- Behebt das Schlüsseltauschproblem
- Ist langsam und rechenintensiv
- Wird meistens benutzt um symmetrische Schlüssel zu tauschen
- Ermöglicht neue kryptographische Methoden (Signieren)
- Großteil der eingesetzten Algorithmen ist nicht PQC tauglich
- Umstellung auf PQC taugliche Algorithmen hätte bereits gestern passieren müssen

Einwegfunktionen - Hashes

4. Einwegfunktionen - Hashes
   - Grundlagen
   - Hash Arten
   - Geburtstagsparadoxon - Angriff
   - Anwendungen

Einwegfunktionen - Hashes

Hashes sind Prüfsummen zum Vergleich von Werten/Daten

4. Einwegfunktionen - Hashes
   - Grundlagen
   - Hash Arten
   - Geburtstagsparadoxon - Angriff
   - Anwendungen

Grundlagen

- Hashes sind Prüfsummen
- Ergebnisse einer Einweg-Funktion
- Unterschiedliche Einsatzzwecke
  - Passworthashes
  - Authentizitätscheck

Eigenschaften

- Unvorhersehbarkeit
- Kollisionsresistenz
- Schnell oder Langsam (nach Einsatzzweck)

Schnelligkeit

Welche Geschwindigkeit wählt man bei welchem Einsatzzweck und warum?

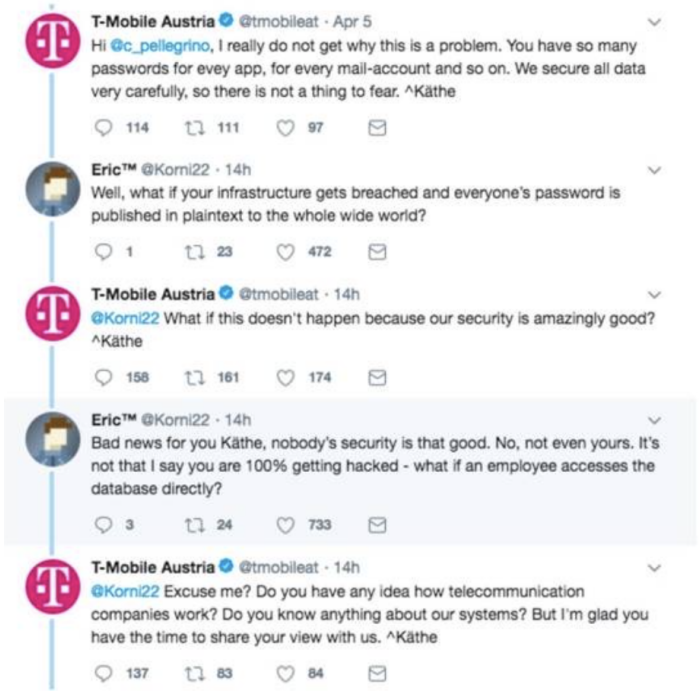
Kollisionshash

- Schnell um Eindeutigkeit einzelner (großer) Daten zu vergleichen
- Beispiele:
  - ~~MD5, SHA1~~[2]
  - SHA 2, SHA 3

[2] `https://shattered.io/`

Passwort-Hash

- „Langsam“ (gegen Brute-Force)
- B-Crypt (from Blowfish)
- Argon 2
- Cheatsheet Password Storing[a]
- Rainbow tables
- Salz und Pfeffer



[a] https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Geburtstagsparadoxon

Gemeinsamer Geburtstag

Es ist wesentlich einfacher in einer Gruppe von Personen ein Paar mit dem selben Geburtstag zu finden, als in der selben Gruppe jemand Zweiten mit einem bestimmten Geburtstag zu finden.

Geburtstagsparadoxon

Gemeinsamer Geburtstag

Es ist wesentlich einfacher in einer Gruppe von Personen ein Paar mit dem selben Geburtstag zu finden, als in der selben Gruppe jemand Zweiten mit einem bestimmten Geburtstag zu finden.

- 50% Wahrscheinlichkeit für ein Paar mit gleichem Geburtstag bei Gruppe von 23 Personen
- n Personen sind $\frac{n(n-1)}{2}$ verschiedene Paare
- Erweitern wir auf $n+1$ Personen kommen n zusätzliche Paarkombinationen hinzu
- Wird verwendet für Kollisionsangriff

Geburtstagsangriff

- Angriff auf jede Hashfunktion möglich
- Bildet Referenzwert für andere Angriffe (muss besser sein als Geburtstagsangriff)
- $p = 1 - (\frac{m}{m} * \frac{m-1}{m} * \frac{m-2}{m} \ldots \frac{m-q+1}{m})$
- $q \approx 1,18 * \sqrt{m}$
- $q =$ Anzahl an Dokumenten die erzeugt werden müssen um 50% Wahrscheinlichkeit für Kollision zu haben
- $m =$ Anzahl an möglichen Hashes
- Bsp.: SHA 1 $\rightarrow 1,18 * 2^{80}$ Versuche benötigt (Bereits anders gebrochen[3])

[3] `https://shattered.io/`

Hash-Tabellen

- Ablöse zu anderen gängigen Indexierungsverfahren (bspw. binary tree)
- Konstanter Zeitaufwand für CRUD Funktionen auch mit wachsender Größe des Index
- Berechne Hash des zu indexierenden Wert und nimm diesen als Index
- Zeitaufwand für CRUD abhängig von gewählter Hash Funktion

Merkle-Tree

- Erfunden 1979 durch Ralph Merkle
- Erweiterung der Hash-Tabelle
- Integritätsschutz
- Anwendung im Integritätsschutz von P2P-Netzen (bspw. Torrents), git, ZFS, Blockchain, etc.
- Bilde Blöcke einer Datei (vgl. Blockchiffren) und hashe diese. Hashe die Hashes der aneinanderliegenden Hashes, usw. bis nur noch ein Top-Hash übrig bleibt.
- Genaue Identifizierung von Fehlern möglich

Blockchain

- Satoshi Nakamoto veröffentlicht 2008 Whitepaper zu Bitcoin
  - Satoshi wird die Cent-Bezeichnung von Bitcoin
  - Satoshi Nakamoto ist Pseudonym. Unbekannt wer dahinter steckt.

Blockchain

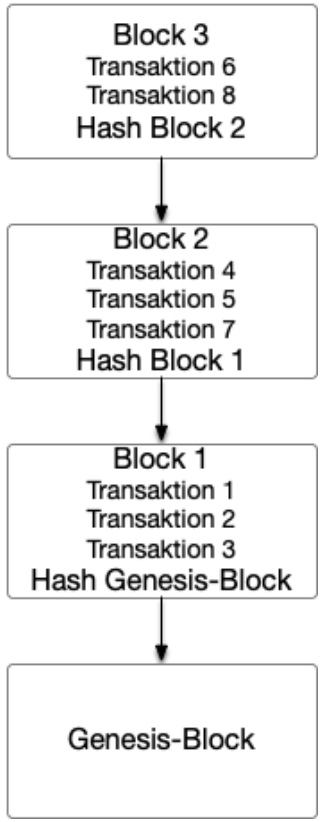
- Satoshi Nakamoto veröffentlicht 2008 Whitepaper zu Bitcoin
  - Satoshi wird die Cent-Bezeichnung von Bitcoin
  - Satoshi Nakamoto ist Pseudonym. Unbekannt wer dahinter steckt.
- Bitcoin ist erste Anwendung der Blockchain und legt Prinzip dessen dar
- Schnell werden weitere Cryptocurrencies geschaffen

Blockchain

- Satoshi Nakamoto veröffentlicht 2008 Whitepaper zu Bitcoin
  - Satoshi wird die Cent-Bezeichnung von Bitcoin
  - Satoshi Nakamoto ist Pseudonym. Unbekannt wer dahinter steckt.
- Bitcoin ist erste Anwendung der Blockchain und legt Prinzip dessen dar
- Schnell werden weitere Cryptocurrencies geschaffen
- Organisationen überlegen diese für weitere Anwendungen zu etablieren. Wenig davon wird wirklich umgesetzt.
- Bekanntes Beispiel außerhalb der Finanzwelt: Certificate Transparency

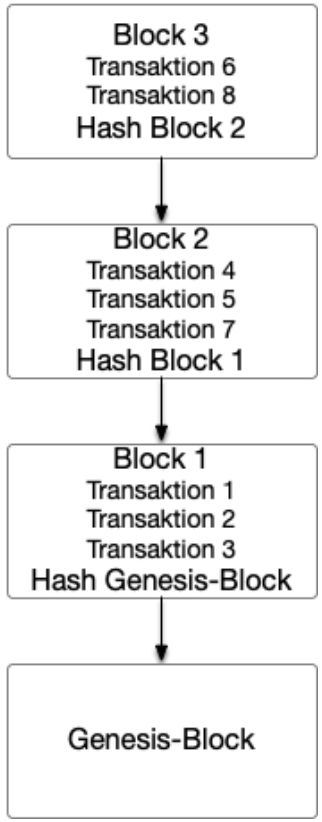
Funktionsweise Blockchain

- Verteilte Datenbank für Transaktionen
- Aneinanderreihung von Blöcken
- Block enthält Transaktionen, Zeitstempel und Merkle-Root des vorigen Blocks
- Erzeugung nach definierten Algorithmus (bspw. genug Transaktionen oder definierte Zeitabstände)



Funktionsweise Blockchain

- Verteilte Datenbank für Transaktionen
- Aneinanderreihung von Blöcken
- Block enthält Transaktionen, Zeitstempel und Merkle-Root des vorigen Blocks
- Erzeugung nach definierten Algorithmus (bspw. genug Transaktionen oder definierte Zeitabstände)

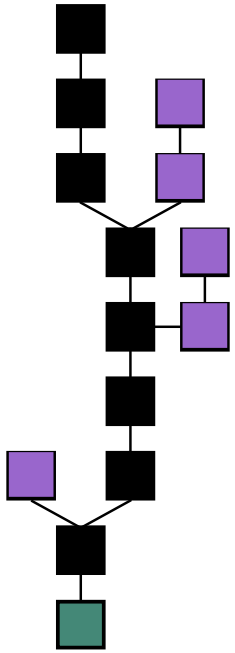


Fragestellung

Was muss ich tun um Daten in einem Block zu verändern?

Dezentralisierung - Verteilung

- Dezentralisierung essentieller Punkt bei Blockchains! (sonst einfach nur Datenbank)
- Verteilung auf mehrere Computer, mit unterschiedlicher Hoheit!
- Einmeldung mehrere nächster Blöcke, jeweiliger Algorithmus entscheidet, welcher angenommen wird (Mining)
- Führt zu verwaisten Blöcken
- 51% Angriff



Fragestellung

Kann ich eine Blockchain auch nicht-verteilt betreiben?

Blockchain Eigenschaften

- Verkettungsprinzip
- Dezentrale Speicherung
- Konsensmechanismus
- Manipulationssicherheit
- Transparenz und Vertraulichkeit
- Nichtabstreitbarkeit

Bitcoin Blockchain Größe

Die Bitcoin Blockchain hat mit Ende 2024 eine Größe von ≈500 GB und wächst pro Jahr um ≈2,5 GB.

Certificate Transparency

- Kontrolle wer welche Zertifikate ausgestellt hat
- Ablöse von CRL und OCSP; läuft schleppend
- CA meldet ausgestelltes Zertifikat in Blockchain ein
- Prüfer durchsucht Blockchain von neunach ältnach dem Zertifikat
- Ist Zertifikat vorhanden (und stimmen die Prüfsummen), ist das vorhandene Zertifikat gültig durch CA ausgestellt
- Automatische Invalidierung alter Zertifikate (neu durch CT!)

Probleme CRL, OCSP, CT

Welche Probleme bringen die jeweiligen Verfahren mit sich?

Anwendungen

5 Anwendungen

- E2EE
- Signalprotokoll - Matrixprotokoll
- Problem: Metadaten
- Shamirs Shared Secret

Anwendungen

Beispielhafte Aufzählung

- Emailverschlüsselung
- Transportverschlüsselung: TLS
  - Bsp. Firefox: TLS_AES_256_GCM_SHA384, 265 bit keys, TLS 1.3
- VPN mit IKE
- Datei und FDE

E2EE - End 2 End Encryption

Was ist E2EE?

E2EE - End 2 End Encryption

Was ist E2EE?

Verschlüsselung und Entschlüsselung passiert am Client. Kein Gateway dazwischen kann den Klartext lesen.

- Implementiert in mehreren Messengern (e.g. Signal, Matrix, Whatsapp, etc.)
- Implementiert in SMIME und PGP
- Oft implementiert in Video und Voicechats

Signalprotokoll

- Erfunden von Signal
- Defacto-Standard für Sofort-Nachrichten
- Wird verwendet von Signal (nonaned), Whatsapp, Facebookmessenger, etc.
- Double-Ratchet-Algorithmus
  - Asymmetrische Schlüssel für den Schlüsseltausch
  - Symmetrische Schlüssel für die Nachrichten
  - Automatischer, regelmäßiger Tausch der Schlüssel (Perfect-Forward-Secrecy)
  - Basiert auf dem Diffie-Hellman
- Matrix benutzt Olm/Megolm (Abkömmling/Variante vom Double-Ratchet)

Signalprotokoll

- Erfunden von Signal
- Defacto-Standard für Sofort-Nachrichten
- Wird verwendet von Signal (nonaned), Whatsapp, Facebookmessenger, etc.
- Double-Ratchet-Algorithmus
  - Asymmetrische Schlüssel für den Schlüsseltausch
  - Symmetrische Schlüssel für die Nachrichten
  - Automatischer, regelmäßiger Tausch der Schlüssel (Perfect-Forward-Secrecy)
  - Basiert auf dem Diffie-Hellman
- Matrix benutzt Olm/Megolm (Abkömmling/Variante vom Double-Ratchet)

Fragestellung

Warum ist die Nutzung von Whatsapp und Facebookmessenger, etc. trotzdem nicht empfohlen?

Problem: Metadaten

Problem: Metadaten

- Quelle/Ziel, Länge/Größe, Dauer/Frequenz, etc.

Problem: Metadaten

- Quelle/Ziel, Länge/Größe, Dauer/Frequenz, etc.
- Metadaten sind meistens nicht verschlüsselt (und können es auch nicht sein)
- Wissen über Metadaten ist genauso wertvoll, wie Wissen über die Payload
- `https://media.ccc.de/v/33c3-7912-spiegelmining_reverse_engineering_von_spiegel-online`
- `https://dkriesel.com/spiegelmining`

Aussagen über Metadaten

- „Metadata absolutely tells you every- thing about somebody's life. If you have enough metadata, you don't really need content." - Stewart Baker, NSA Counsel
- „We kill people based on metadata." - Former NSA Director Michael Hayden
- Beispiel Ukraine Funkverkehr:
  - Unverschlüsselt kann Militärisch sein
  - Verschlüsselt ist recht sicher militärisch
  - Ist es mein oder verbündetes Militär?
  - Nein $\rightarrow$ Raketenschlag
- Einwahl mehrerer russischer SIM Karten $\rightarrow$ Truppenansammlung

Shamirs Shared Secret

- Teile den Schlüssel in mehrere Teile (Shares)
- Mehrere Teile sind benötigt um zu entschlüsseln (Threshold). Anzahl ist auswählbar.
- Beispiel: Teile den Schlüssel in vier Teile und verteile diese an vier Personen. Drei Personen sind notwendig um den Schlüssel zu benutzen.

Kryptoanalyse

Kryptoanalyse

Wege um die Kryptographie zu brechen:

- Bruteforce
- Side-Channel-Attacks
- Wissen über den Algorithmus erforderlich
  - Best Practice: Open-Source
  - Ansonsten Ziel von Spionage
- Angriff auf den Algorithmus (bspw. mathematische Schwachstelle)
- Angriff auf die Implementierung (bspw. fehlerhafte Programmierung)
- Angriff auf den User (bspw. Phishing)

Kryptoanalyse

Wege um die Kryptographie zu brechen:

- Bruteforce
- Side-Channel-Attacks
- Wissen über den Algorithmus erforderlich
  - Best Practice: Open-Source
  - Ansonsten Ziel von Spionage
- Angriff auf den Algorithmus (bspw. mathematische Schwachstelle)
- Angriff auf die Implementierung (bspw. fehlerhafte Programmierung)
- Angriff auf den User (bspw. Phishing)
- $\rightarrow$ Lebensdauer und Kritikalität der Information bestimmt das erforderliche Security-Level

Ausblick

Ausblick

- Homomorphe Verschlüsselung $\rightarrow$ Heilige Gral
- Durchsuchbare Verschlüsselung

Zusammenfassung

Zusammenfassung

- NIEMALS! eine eigens gebaute (unter Verschluss gehaltene) Kryptographie verwenden. (Bsp. Tetra - Behördenfunk)
- Lebensdauer und Kritikalität der Information bestimmt das erforderliche Security-Level
- Fähigkeiten der Angreifer (nicht der User) bestimmen das benötigte Security-Level
- Im Zweifel: Beste verfügbare Algorithmen und Modi verwenden
- CIA - Confidentiality, Integrity, Availability
- SUE - Security, Usability, Economy/Ecology