KRYPTOLOGIE UND SYSTEMSICHERHEIT

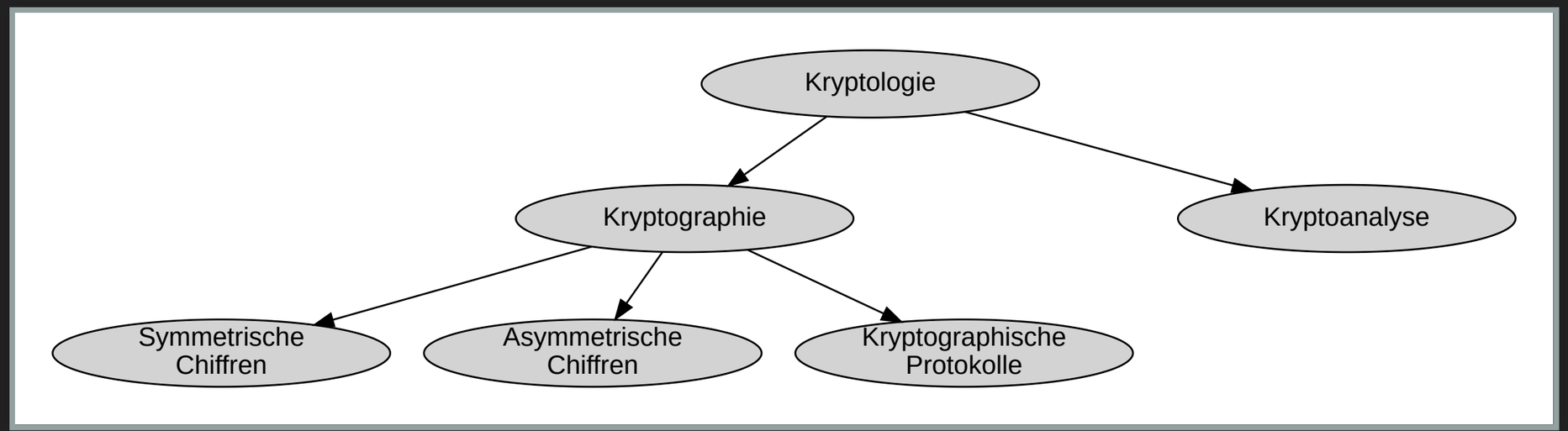
Sommersemester 2020

Technische Hochschule Mittelhessen

Andre Rein

– Kryptologie Einführung –

GRUNDLAGEN


Kryptologie
Kryptographie
Kryptoanalyse
Symmetrische Chiffren
Asymmetrische Chiffren
Kryptographische Protokolle

KRYPTOGRAPHIE

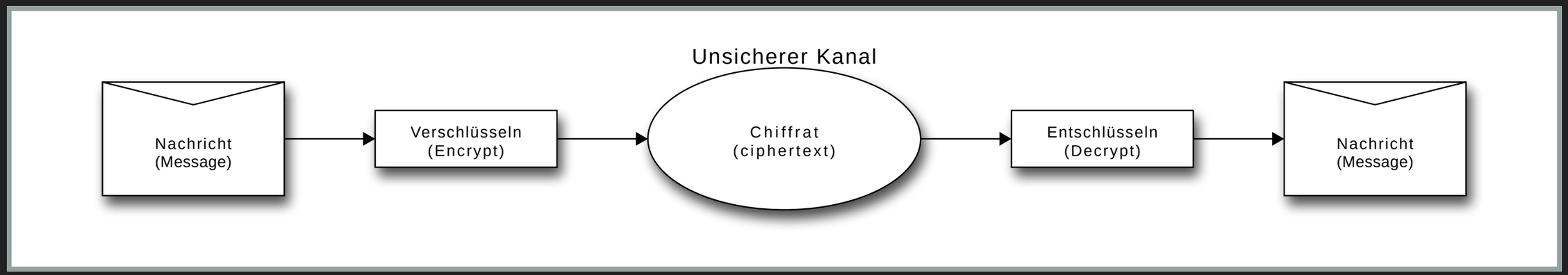
Die Kryptographie beschäftigt sich mit der Absicherung von Daten. (Z.B. der Verschlüsselung von Nachrichten.)

TEILGEBIETE DER KRYPTOGRAPHIE

- **Symmetrische Chiffren**
  - Bekannteste und intuitivste Form der Kryptographie
  - Die gesamte Kryptographie von der Antike bis 1976 basiert auf symmetrischen Chiffren
- **Asymmetrische Chiffren (Public-Key)**
  - Eingeführt 1976 von Diffie, Hellman, Merkle
  - Basiert primär auf spezifischen mathematischen Eigenschaften und Strukturen
  - Verwendet einem privaten (private) und einem öffentlichen (public) Schlüssel
- **Kryptographische Protokolle**
  - Sind entweder eigenständige Verfahren um bestimmte kryptographische Probleme zu lösen (z.B. Schlüsseltausch, Schlüsselverteilung, …)
  - Oder, verwenden symmetrische und asymmetrische Methoden um komplexere Systeme / Verfahren zu implementieren (z.B. TLS (verwendet bspw. in HTTPS))

VERSCHLÜSSELUNG UND ENTSCHLÜSSELUNG VON DATEN

- Per Definition liegt eine Nachricht (Message) im **Klartext** (**Plaintext**) vor
  - Nachricht ← → Daten → Beliebiger Strom von Bits
- Die Verschleierung des Inhalts einer Nachricht wird **Verschlüsselung** (Encryption) genannt
- Das Resultat der Verschlüsselung einer Nachricht wird als **Ciphertext** (Chiffrat) bezeichnet
- Der Prozess, einen Chiffretext wieder in Klartext zu verwandeln, wird als **Entschlüsselung** (Decryption) bezeichnet



VERSCHLÜSSELUNG UND ENTSCHLÜSSELUNG VON DATEN

- Eine Nachricht im Klartext wird mit M gekennzeichnet
- Ciphertext wird mit C gekennzeichnet
- Die Verschlüsselungsfunktion E wird angewendet auf M und erzeugt C
  - Es gilt: $E(M) = C$
- Die Entschlüsselungsfunktion D wird angewendet auf C und erzeugt M
  - Es gilt: $D(C) = M$
- Die Entschlüsselung einer verschlüsselten Nachricht erzeugt wieder die Nachricht
  - Es gilt: $D(E(M)) = M$

VERSCHLÜSSELUNG UND ENTSCHLÜSSELUNG VON DATEN

Nehmen Sie an Sie möchten Daten verschlüsseln und komprimieren:

- Welche Reihenfolge ist richtig?
  - Erst verschlüsseln, dann komprimieren
  - Erst komprimieren, dann verschlüsseln

ANTWORT:

Die Komprimierung von Daten basiert auf Redundanz innerhalb der Originalquelle (loose) oder dem Verzicht auf unwesentliche Details aus der Quelle (loosy)

- Ziel von Verschlüsselung ist es Daten zu einer zufällig aussehenden Bitreihenfolge zu transformieren
- Entfernen von unwesentlichen Details ist in verschlüsselten Daten nicht möglich (loosy)
- Redundanzen innerhalb verschlüsselter Daten sind somit ebenfalls zufällig, da die Strukturen ebenfalls verborgen sein sollten (loose)
  - Eine Komprimierung wäre dann möglich, aber eher ineffektiv und zufällig

Erst komprimieren, dann verschlüsseln!

ALGORITHMEN UND SCHLÜSSEL

AUFGABE: KERCKHOFFS'SCHE PRINZIP ✍

- Recherchieren Sie online was es mit dem Begriff **Kerckhoffs'sche Prinzip** auf sich hat
- Recherchieren Sie zusätzlich dazu in welchem Zusammenhang dies mit sog. **eingeschränkten** und **uneingeschränkten Algorithmen** steht
- Sprechen und diskutieren Sie über den Begriff / die Themen mit Ihren Nachbarn
- Notieren Sie sich kurz zu den Begriffen, was Sie bedeuten und welche Konsequenz dadurch für die Kryptographie besteht.

- ⏱ Bearbeitung: 15 Minuten!

EINGESCHRÄNKTE ALGORITHMEN (RESTRICTED ALGORITHMS)

Security through Obscurity

- Ein kryptographischer Algorithmus (**cipher**) ist eine (*umkehrbare*) **mathematische Funktion**, die zur Ver- und Entschlüsselung verwendet wird
- Wenn der Algorithmus selbst geheim gehalten wird und seine Sicherheit auf dieser Geheimhaltung basiert, wird er als **eingeschränkter Algorithmus** bezeichnet
- Eingeschränkte Algorithmen sind nur von historischem Interesse:
  - Verlässt ein Benutzer eine Gruppe die den Algorithmus kennt, muss der Algorithmus geändert werden
  - Wird der Algorithmus aufgedeckt (versehentlich oder nicht), muss jeder, der ihn verwendet, den Algorithmus ändern
  - Es gibt keine Qualitätskontrolle oder Standardisierung → Das bedeutet, dass der Algorithmus möglicherweise nicht richtig untersucht wurde

UNEINGESCHRÄNKTE ALGORITHMEN (UNRESTRICTED ALGORITHMS)

- Moderne Kryptographie überwindet diese Probleme durch die Verwendung eines **Schlüssels** K
- Der Bereich der möglichen Werte des Schlüssels ist der **Schlüsselraum**
- Der Algorithmus ist so entworfen das die gesamte Sicherheit des **Kryptosystems** nur auf dem Schlüssel selbst basiert
  - Der Algorithmus kann veröffentlicht und analysiert werden
  - Solange der Schlüssel einem Angreifer unbekannt ist, können verschlüsselte Nachrichten nicht gelesen werden
  - Voraussetzung: Algorithmus ist sicher und nicht gebrochen + Schlüssellänge ist ausreichend groß gewählt

DAS KERCKHOFFS'SCHE PRINZIP

Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.

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

La cryptographie militaire 1883
— Auguste Kerckhoffs

DAS KERCKHOFFS'SCHE PRINZIP

- Es ist viel schwieriger, einen Algorithmus geheim zu halten als einen Schlüssel
- Es ist schwieriger, einen Algorithmus durch einen anderen zu ersetzen als einen kompromittierten Schlüssel
- Geheime Algorithmen können durch Reverse Engineering aus Software- oder Hardware-Implementierungen rekonstruiert werden
- Fehler in öffentlichen Algorithmen werden leichter entdeckt (Peer-Review), wenn sich möglichst viele Fachleute damit befassen
- Es ist leichter, in "geheimen" Verschlüsselungsverfahren eine Hintertür zu verstecken

Quelle: https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip

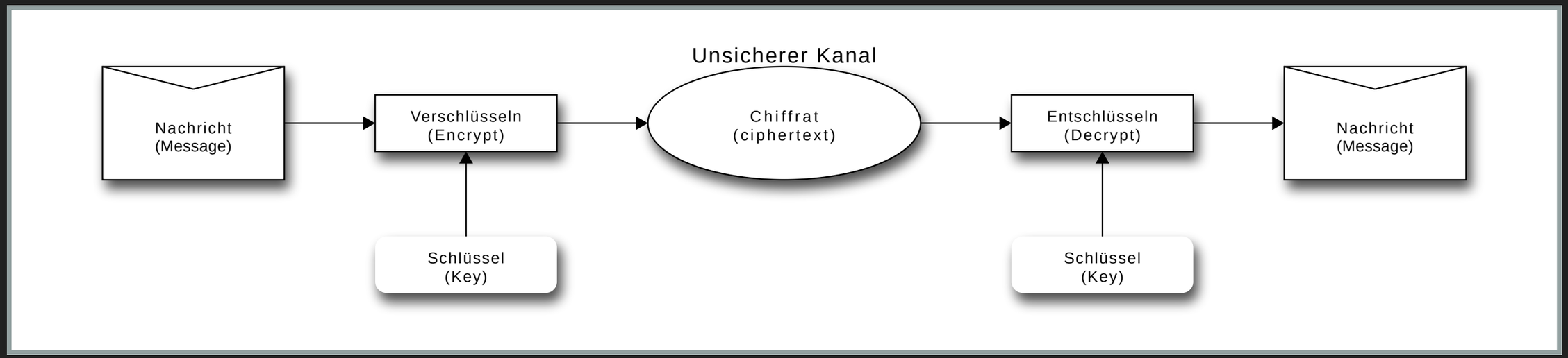
UNEINGESCHRÄNKTE ALGORITHMEN

Ein Schlüssel K für Verschlüsselung und Entschlüsselung

Verschlüsselung $E_K(M) = C$

Entschlüsselung $D_K(C) = M$

Eigenschaft $D_K(E_K(M)) = M$



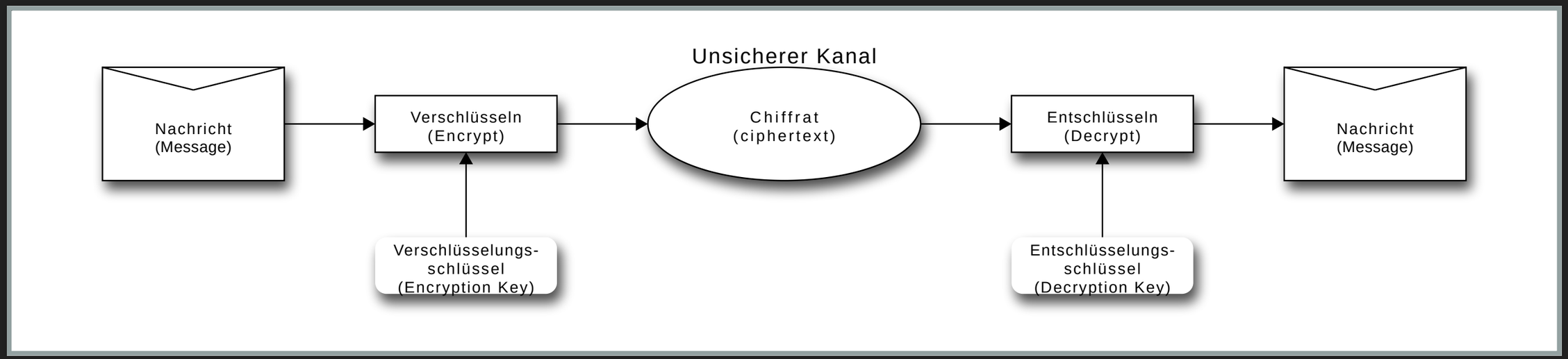
UNEINGESCHRÄNKTE ALGORITHMEN

Ein Schlüssel K_1 für Verschlüsselung und ein anderer Schlüssel K_2 für Entschlüsselung

Verschlüsselung $E_{K_1}(M) = C$

Entschlüsselung $D_{K_2}(C) = M$

Eigenschaft $D_{K_2}(E_{K_1}(M)) = M$



SYMMETRISCHE ALGORITHMEN

- Symmetrische Algorithmen verwenden typischerweise einen Schlüssel für die Ver- und Entschlüsselung
  - Werden auch als Secret-Key-Algorithmen oder Single-Key-Algorithmen bezeichnet
- Es zwei Kategorien (wird später näher erläutert):
  - Stromchiffren
  - Blockchiffren
- Beliebte Algorithmen: AES, DES, Blowfish, Serpent, IDEA, eStream, …

ASYMMETRISCHE (PUBLIC KEY) ALGORITHMEN

- Asymmetrische Algorithmen werden auch als Public-Key-Algorithmen bezeichnet
- Sie benutzen zwei unterschiedliche Schlüssel — Einen für die Verschlüsselung und eine für die Entschlüsselung
  - Der **Entschlüsselungsschlüssel** wird als privater Schlüssel bezeichnet und bleibt geheim
  - Der **Verschlüsselungsschlüssel** wird als öffentlicher Schlüssel bezeichnet und kann öffentlich zugänglich gemacht werden
- Beide Schlüssel stehen in mathematischer Beziehung

	Eigenschaft: Der private Schlüssel kann nicht effizient aus dem öffentlicher Schlüssel berechnet werden

ASYMMETRISCHE (PUBLIC KEY) ALGORITHMEN

NOTATION FÜR ASYMMETRISCHE ALGORITHMEN

Verschlüsselung $E_{pub}(M) = C$

Entschlüsselung $D_{priv}(C) = M$

Eigenschaft $D_{priv}(E_{pub}(M)) = M$

- Beliebte Algorithmen und Verfahren: RSA, DSA, ElGamal, Diffie-Hellman-Key-Exchange, Elliptic-Curve-Cryptography, …
- Asymmetrische Algorithmen werden auch für digitale Signaturen verwendet
  - In diesem Fall erfolgt die Verschlüsselung mit dem privaten Schlüssel und die Entschlüsselung mit dem öffentlichen Schlüssel

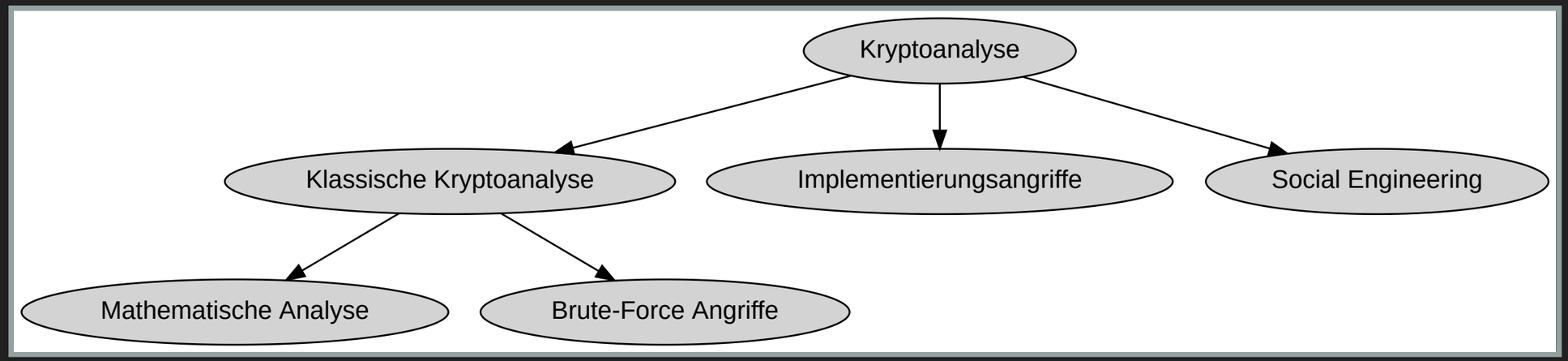
Fragen?

KRYPTOANALYSE

Die Kryptoanalyse bei Verschlüsselungssystemen ist die Wissenschaft der Gewinnung an Informationen einer verschlüsselten Nachricht ohne Kenntnis des geheimen Schlüssels (oder anders gesagt, dem Brechen eines Kryptosystems) Es ist außerdem der Hauptansatz mit der die Sicherheit eines kryptographischen Verfahrens bewertet wird!

	Ein erfolgreicher Angriff bedeutet, dass entweder der Klartext, Teile des Klartextes oder der geheime Schlüssel bekannt wird

KRYPTOANALYSE



- Implementierungsangriffe: Schlüsselgewinnung durch Reverse-Engineering oder Seitenkanalangriffe
- Social Engineering: z.B. Täuschung eines Benutzers der sein Passwort verrät

KRYPTOANALYSE: BRUTE FORCE ANGRIFF

- Man benötigt mindestens ein Klartext (x_0) und ein Chiffrat (y_0)
- Chiffre wird als Blackbox betrachtet
- Testen aller möglichen Schlüssel ($\forall K \in \{0,1\}^n \rightarrow$ ausführliche/vollständige Schlüsselsuche) bis Bedingung erfüllt ist:

$$D_K(y_0) = x_0$$

KRYPTOANALYSE: BRUTE FORCE ANGRIFF FRAGE

Frage: Wie groß sollte n gewählt werden damit ein Brute Force Angriff ineffizient wird?

90 BIT GILT HEUTE ALS SICHER!

KRYPTOANALYSE: PASSWÖRTER (AUFGABE 4.1)✍

FRAGE: WELCHE BITSICHERHEIT HAT EIN PASSWORT ...

1. mit nur Klein/Großbuchstaben und Ziffern (0-9) ohne Umlaute mit der Länge von 16 Zeichen?
2. mit 5 zufällig gewählten ASCII-Zeichen (d.h. je 256 mögliche Zeichen)
3. mit 12 zufällig gewählten ASCII-Zeichen (d.h. je 256 mögliche Zeichen)

⏱ Bearbeitung: 5 Minuten → dann diskutieren!

KRYPTOANALYSE: MATHEMATISCHE ANALYSE

- Viele kryptographische Algorithmen basieren auf mathematischen Problemstellungen die nicht **effizient** algorithmisch lösbar sind
  - Nicht effizient bezieht sich hierbei auf: Rechenzeit oder Speicherbedarf
- Beispiel Primfaktorzerlegung: Faktorisierungsproblem von großen ganzen Zahlen
  - Vermutung: Lässt nicht nicht in polynomialer Zeit lösen
  - *Dies ist jedoch nicht endgültig bewiesen!*

	Algorithmen die auf mathematisch ungelösten Problemen basieren sind sicher bis das mathematische Problem gelöst ist

KRYPTOANALYSE: STRUKTURELLE ANALYSE

Neben der mathematischen Analyse kann auch eine Analyse der internen Struktur des Kryptosystems durchgeführt werden. Hier gibt es verschiedene Ansätze die wir später betrachten.

Ein einfaches Verfahren ist die sog. Frequenz- oder Häufigkeitsanalyse. Diese schauen wir uns gegen Ende genauer an.

BEISPIEL: EINFACHE MONOALPHABETISCHE SUBSTITUTION

- Ziel → Verschlüsselung eines Textes
- Idee → Jeder Buchstabe aus dem Alphabet wird durch einen beliebigen anderen Buchstaben des Alphabets ersetzt (keine Dopplungen!)

- A → K
- B → X
- C → F
- ...

FRAGE: IST EIN BRUTE FORCE ANGRIFF MÖGLICH?

- Nein: Denn es gibt 2^{88} mögliche Schlüssel
  - $26 * 25 * 24... * 3 * 2 * 1 = 26! \approx 2^{88}$

KRYPTOANALYSE FÜR MODERNER KRYPTOGRAPHIE

Alle aktuelle und moderne Verfahren die wir in der Veranstaltung besprechen basieren auf Problemen für die zumindest bis heute keine effizienten Algorithmen bekannt sind, die wesentlich *besser* sind als ein Brute-Force Angriff.

Alle Algorithmen sind seit vielen Jahren bekannt und wurden hinsichtlich mathematischer Schwächen hinreichend untersucht!

	Trotzdem kann die falsche Verwendung oder Kombination von Verfahren dazu führen, dass das Kryptosystem nicht als sicher betrachtet werden kann! Details folgen im Laufe des Semester.

ALGORITHMUS-SICHERHEIT

Total Break	Ein Kryptoanalytiker findet den Schlüssel K für $D_K(C) = M$
Global Deduction	Ein Kryptoanalytiker findet einen Algorithmus A der $D_K(C) = M$ löst, ohne K zu verwenden
Local Deduction	Ein Kryptoanalytiker findet den Klartext zu **einem** bestimmten Ciphertext
Information Deduction	Ein Kryptoanalytiker erlangt Information über den Schlüssel oder den Klartext. (Einige Bits des Schlüssels / Informationen zum Klartext [z.B. Strukturen])

ALGORITHMUS-SICHERHEIT

- Ein **Kryptosystem** ist **uneingeschränkt sicher** (unconditionally secure), wenn es selbst mit unendlich viel Rechenleistung nicht gebrochen werden kann

	Es gibt nur ein Kryptosystem das auch bei der Annahme von unendlichen Ressourcen diese Eigenschaft besitzt

- Alle anderen Kryptosysteme sind (einfach) zu brechen, indem man alle möglichen Schlüssel ausprobiert
- Kryptosysteme gelten als sicher, wenn sie **nicht** in **effizienter** Weise, d.h. in angemessener Zeit, gebrochen werden können

WENN DER VERWENDETE ALGORITHMUS KEINE (BEKANNTEN) SCHWÄCHEN HAT UND SOMIT KEIN ANDERER ANGRIFF BEKANNT IST, DER SCHNELLER ALS BRUTE-FORCE IST, DEFINIERT DIE VERWENDETE SCHLÜSSELLÄNGE DAS SICHERHEITSNIVEAU DES KRYPTOSYSTEMS UND DAS VERFAHREN GILT ALS SICHER!

SCHLÜSSELLÄNGE BESTIMMTER VERFAHREN

DES	2^{56} = 72.057.594.037.927.936 (entspricht 56 Bit)
Enigma I	103.325.660.891.587.134.000.000 (entspricht ungefähr 76 Bit)
Enigma-M4	60.176.864.903.260.346.841.600.000 (entspricht fast 86 Bit)
Monoalphabetische-Substitution	$26!$(Fakultät) = 403.291.461.126.605.635.584.000.000 (entspricht ungefähr 88 Bit)
Triple-DES	2^{112} = 5.192.296.858.534.827.628.530.496.329.220.096

SCHLÜSSELLÄNGE BESTIMMTER VERFAHREN

AES-128	2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456
AES-192	2^{192} = 6.277.101.735.386.680.763.835.789.423.207.666.416.102.355.444.464.0
AES-256	2^{256} = 115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.

SCHLÜSSELLÄNGEN EMPFEHLUNGEN (NIST 2019)

Date	Security Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm		Elliptic Curve	Hash (A)	Hash (B)
				Key	Group			
Legacy [1]	80	2TDEA	1024	160	1024	160	SHA-1 [2]	
2019 - 2030	112	(3TDEA) [3] AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512, KMAC256

http://www.keylength.com/

2TDEA - 2 unabhängige Schlüssel, 3TDEA - 3 unabhängige Schlüssel

AUFGABEN: HÄUFIGKEITSANALYSE UND MONOALPHABETISCHE SUBSTITUTION

BEISPIEL: KURZEINFÜHRUNG EINFACHE MONOALPHABETISCHE SUBSTITUTION

- Obwohl ein Brute Force Angriff auf die einfache monoalphabetische Substitution nicht effizient ist, ist das Verfahren trotzdem sehr schwach
- Es kann mit Hilfe einer Fequenz-/Häufigkeitsanalyse sehr einfach gebrochen werden

- `E` kommt am häufigsten vor → Ersetze häufigsten Buchstaben im Chiffrat mit `E`
- `N` kommt am zweithäufigsten vor → Ersetze zweithäufigsten Buchstaben mit `N`
- auf `C` folgt oft ein `H`, auf `Q` folgt fast immer ein `U`, …

🔥	Die statistischen Häufigkeiten zwischen Klartext und Chiffrat werden nicht verborgen

	Ein gutes Verschlüsselungsverfahren verbirgt **alle Abhängigkeiten**

KRYPTOANALYSE: HÄUFIGKEITSANALYSE ✍️

- **Aufgabe 1**: Ziel der ersten Aufgabe ist es ein Programm zu entwickeln, das eine Häufigkeitsanalyse eines Textes ausführt und die statistische Buchstabenverteilung ausgibt.
  - Bearbeiten Sie die Aufgabe Frequency Analyzer.
- **Aufgabe 2**: Entschlüsseln Sie das Chiffrat und geben Sie den Klartext an.
  - Bearbeiten Sie hierzu die Aufgabe Monoalphabetic Substitution.

⏱️ Bearbeitung: Rest der Stunde + Hausaufgabe :) Besprechen wir das nächste mal!