9. Einführung in die Kryptographie

Grundidee: A sendet Nachricht nach B über unsicheren Kanal. Es soll verhindert werden, dass ein Unbefugter Kenntnis von der übermittelten Nachricht erhält.

Grundbegriffe:

Kryptographie: Wissenschaft von der Verschlüsselung von Daten. Ein Kryptograph entwickelt kryptographische Verfahren zur Verschlüsselung von Daten.

Krypt(o)analyse: Analyse von verschlüsselten Daten. Das Ziel eines Kryptoanalytiker ist es, eine verschlüsselte Nachricht zu knacken.

Kryptoanalytiker, Angreifer: jemand, der versucht, ein kryptographisches System anzugreifen, z. B. mit Hilfe von Kryptoanalyse.

Angriff, *Attacke*: Versuch, eine verschlüsselte Botschaft zu entschlüsseln, d. h. lesbar zu machen ("knacken").

Chiffrierung: Synonym für Verschlüsselung

Dechiffrierung: Synonym für Entschlüsselung.

Chiffretext, *Geheimtext*: Resultat der Verschlüsselung.

Klartext: der unverschlüsselte Text.

9.1 Transpositionschiffren

Buchstaben bleiben, was sie sind, aber nicht wo sie sind.

Beispiel (in Sparta ungefähr 2500 v. Chr. benutzt)

Sender wickelt schmales Band aus Pergament spiralförmig um Zylinder mit bestimmtem Radius und schreibt Nachricht auf das Band. Nachricht wird abgewickelt und an Empfänger geschickt. Hat dieser Zylinder mit demselben Radius, kann er die Nachricht lesen.

H A L L O L E U T E W I E G E H T E S E U C H

Wir verschlüsseln nun diesen Text mit einem Zylinder des Umfangs U = 5, indem wir den Text in 5 Spalten aufteilen:

H A L L O
L E U T E
W I E G E
H T E S E
U C H

Das Ergebnis ergibt sich, indem man jede Spalte dieses Textes von oben nach unten liest und alles hintereinander aufschreibt:

H L W H U A E I T C L U E E H L T G S O E E E

Diese Art der Transposition wird auch Spaltentransposition genannt.

Transposition (auch Permutation genannt) alleine ist nicht sicher.

9.2 Verschiebechiffren

schon von Julius Caesar benutzt.

Klartextalphabet über das *Geheimtextalphabet* schreiben – aber um *k* Stellen verschoben. Beispiel:

Klartext: 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

Geheimtext: 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

Hier wurde Geheimtextalphabet um 3 Stellen nach links verschoben.

Man chiffriert Nachricht, indem man Klartextbuchstaben durch darunter stehenden Geheimtextbuchstaben ersetzt.

Aus dem Wort LEIPZIG würde in unserem Fall OHLSCLJ.

Für *k* genau 26 Möglichkeiten (wobei k = 26 nicht sehr sinnvoll!).

Verfahren leicht zu knacken.

Solche Chiffrierungen werden auch als *additive* Chiffrierungen bezeichnet: Code des n-ten Klartextbuchstabens ist der (n + k)te Buchstabe, falls (n + k) > 26 der (n + k - 26)ste.

9.3 Multiplikative Chiffren

Bei dieser Chiffrierung verwendet man statt Addition Multiplikation modulo 26. (Positionen werden ebenfalls modulo 26 gezählt, also die von z ist 0!).

jeder Klartextbuchstabe mit dem Schlüssel *k* multipliziert. Beispiel mit *k* = 2:

Klartext: 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

Geheimtext: B D F H J L N P R T V X Z B D F H J L N P R T V X Z

jeweils zwei unterschiedliche Buchstaben ergeben dasselbe Produkt!

nicht als Chiffre verwendbar.

Klartext muss mit Hilfe des Schlüssels ***eindeutig*** *aus dem Geheimtext rekonstruierbar sein!*

k = 3:

Klartext: 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

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

Diese Chiffrierung funktioniert! ebenso mit 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 und 25.

Diese Zahlen haben keine gemeinsamen Teiler mit 26! 26 ist das Produkt der beiden Primzahlen 2 und 13, wir dürfen keine Zahlen verwenden, die ein Vielfaches von 2 oder 13 sind (Zahlen müssen *teilerfremd* zu 26 sein).

Für diese Art der Chiffrierung gibt es somit nur exakt 12 Möglichkeiten.

9.4 Monoalphabetische Chiffrierungen

Verfahren, bei denen jeder Buchstabe des Alphabets zu demselben Geheimtext-Buchstaben verschlüsselt wird, heißen monoalphabetisch (Verschiebechiffren und multiplikative sind Spezialfälle):

Klartext: 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
Geheimtext: Q A Y W S X E D C R F V T G B Z H N U J M I K O L P

$26 \cdot 25 \cdot 24 \cdot ... \ 3 \cdot 2 \cdot 1 = 26! = \sim 4 \cdot 1026$ Möglichkeiten!
trotzdem meist leicht zu knacken.

Das Entziffern von monoalphabetischen Chiffren erleichtert durch Häufigkeitsanalyse:

Häufigkeiten der Buchstaben in der deutschen Sprache:

Buchstabe	**Häufigkeit in %**	**Buchstabe**	**Häufigkeit in %**
a	6,51	n	9,78
b	1,89	o	2,51
c	3,06	p	0,79
d	5,08	q	0,02
e	17,40	r	7,00
f	1,66	s	7,27
g	3,01	t	6,15
h	4,76	u	4,35
i	7,55	v	0,67
j	0,27	w	1,89
k	1,21	w	1,89
l	3,44	y	0,04
m	2,53	z	1,13

Quelle: Albrecht Beutelspacher, Kryptologie

Häufigkeit des Auftretens eines Symbols in Chiffre lässt Rückschlüsse zu!

9.5 Polyalphabetische Chiffrierungen

Klartextbuchstabe wird nicht stets mit demselben Geheimtextbuchstaben verschlüsselt.

Nachteil bei monoalphabetischen Chiffren: Buchstabenhäufigkeiten nicht verborgen.

a) Ordne einem Klartextbuchstaben nicht nur *ein*, sondern *mehrere* Geheimtextzeichen zu! Anzahl der Geheimtextzeichen sollte Häufigkeit des Klartextbuchstabens entsprechen.

z. B.: e (Häufigkeit: ca. 17%) 17 Geheimtextzeichen von 100 Paaren 00 bis 99 zugewiesen

Beispiel:

a: 10 21 52 59 71
b: 20 34
c: 28 06 80
d: 04 19 70 81 87
e: 09 18 33 38 40 42 53 54 55 60 66 75 85 86 92 93 99
f: 00 41
g: 08 12 97
h: 07 24 47 89
i: 14 39 46 50 65 76 88 94
j: 57
k: 23
l: 16 03 84
m: 27 11 49
n: 30 35 43 62 63 67 68 72 77 79
o: 02 05 82
p: 31
q: 25
r: 17 36 51 69 74 78 83
s: 15 26 45 56 61 73 96
t: 13 32 90 91 95 98
u: 29 01 58
v: 37
w: 22
x: 44
y: 48
z: 64

aus: Albrecht Beutelspacher, Kryptologie

Chiffrieren: ordne jedem Klartextbuchstaben zufällig gewähltes Zeichen aus der Menge der möglichen Geheimtextzeichen für diesen Buchstaben zu.

Jeder Buchstabe des Geheimtextes tritt mit etwa der gleichen Häufigkeit auf.

b) Die Vigenère-Chiffre

von Blaise de Vigenère, wurde 1586 veröffentlicht.

Zum Chiffrieren (a) ein **Schlüsselwort** und (b) das **Vigenère-Quadrat**:

```
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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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
```

Quadrat aus 26 Alphabeten, erste Zeile um 0 Stellen verschoben, zweite um 1 Stelle verschoben, letzte um 25 Stellen verschoben. Schlüsselwort kann eine beliebige Buchstabenfolge sein, z. B. das Wort `KRYPTO`.

Wir schreiben nun dieses Schlüsselwort unter den Klartext und wiederholen es, wenn nötig:

Der Schlüsselbuchstabe, der unter einem Klartextbuchstaben steht, bestimmt das Alphabet. Allgemein: Um Klartextbuchstaben *p* mit dem Schlüsselbuchstaben *k* zu verschlüsseln, sieht man im Vigenère-Quadrat nach, was in der Zeile *k* und in der Spalte *p* steht:

```
Klartext:      p o l y a l p h a b e t i s c h
Schlüsselwort: K R Y P T O K R Y P T O K R Y P
Geheimtext:    Z F J N T Z Z Y Y Q X H S J A W
```

Um Geheimtext zu entschlüsseln, suchen wir in der Zeile *k* nach dem Geheimtextbuchstaben *c* und prüfen, in welcher Spalte *c* steht. Diese liefert Klartextbuchstaben (oberste Zeile).

Häufigkeit der Buchstaben gleichmäßiger verteilt: Die beiden a im Klartext werden zu unterschiedlichen Geheimtextbuchstaben verschlüsselt (nämlich T und Y).

Auch diese Chiffrierung mit heutigen Methoden leicht zu knacken.

9.6 Moderne Verfahren: Data Encryption Standard (DES)

moderne Algorithmen verarbeiten Bits.
Häufiger Bestandteil *xor*: 0 xor 0 = 0, 0 xor 1 = 1, 1 xor 0 = 1, 1 xor 1 = 0.
Sei s ein binärer Schlüssel, dann gilt: y = x xor s gdw. x = y xor s
Beispiel: 10001 xor 00101 = 10100, 10100 xor 00101 = 10001

DES (IBM) 1977 zum Standard erklärt.

- verschlüsselt jeweils Blöcke von 64 Bit Länge (Blockalgorithmus)
- Block nach Eingangspermutation in zwei Hälften L und R der Länge 32 Bit aufgeteilt.
- Blöcke durchlaufen 16 Runden, in jeder Runde wird R expandiert auf 48 Bit, XOR mit aktuellem Schlüssel, Ergebnis in 8 Blöcke a 6 Bits aufgeteilt, diese jeweils anhand verschiedener Tabellen in 4 Bits umgewandelt. Die so entstandenen 32 Bit werden permutiert und es wird XOR mit L durchgeführt. Das Ergebnis wird dem R-Register zugewiesen, der alte Wert von R in L übernommen.
- Nach 16 Runden werden L und R wieder zusammengeführt und nochmals permutiert.
- Der in einer Runde verwendete 48-Bit-Schlüssel wird jeweils aus dem ursprünglichen 64-Bit-Schlüssel generiert (Entfernen von 8 Paritätsbits, Permutation, Spalten in 2 Hälften mit jeweils 28 Bit, Rotieren der Hälften, Auswahl der 48 verwendeten Schlüsselbits).
- Aufgrund der Verwendung von XOR kann derselbe Algorithmus zum Codieren und zum Decodieren verwendet werden.
- Recht sicher: jedes Eingangsbit hat Einfluss auf jedes Ausgangsbit, Änderung eines Eingangsbits verändert etwa 50% der Ausgangsbits.
- Heute verwendete Verfahren verwenden längere Schlüssel.

Anmerkung:

bisher vorgestellte Techniken benutzen selben Schlüssel für Chiffrierung und Dechiffrierung.
Sie werden deshalb auch als *symmetrische* Verfahren bezeichnet.
Nachteil: Schlüssel muss an Nachrichtenempfänger übermittelt werden.

Asymmetrische Verfahren (public key Verfahren) kommen ohne Schlüsselaustausch aus:

- Alice verschlüsselt Nachricht mit Schlüssel k_A und schickt sie an Bob;
- Bob codiert von Alice verschlüsselte Nachricht mit Schlüssel k_B und schickt sie zurück;
- Alice entschlüsselt erhaltene Nachricht mit k_A und schickt Resultat wieder an Bob;
- Bob entschlüsselt erhaltene Nachricht mit k_B.

Es gibt Methoden, die ohne mehrfaches Hin- und Hersenden auskommen -> Hauptstudium