b) Substitutionschiffren

Bei Substitutionsverfahren werden die Zeichen einer Nachricht durch andere ersetzt aber innerhalb der Nachricht nicht anders angeordnet.

Typ 1: Monoalphabetische Substitution

Unter monoalphabetischen Substitutionen versteht man Verfahren, bei denen jeder Buchstabe des Klartext-Alphabets zu demselben Geheimtext-Buchstaben verschlüsselt wird. Man kann z.B. jedem Buchstaben ein bestimmtes Zeichen (oder einen anderen Buchstaben) zuordnen.

Beispiele: Caesar-Code, Atbasch, Playfair, Morse-Code

Typ 2: Polyalphabetische Substitution

Bei der polyalphabetischen Substitution wird derselbe Klartextbuchstabe nicht stets mit demselben Geheimtextbuchstaben verschlüsselt. Bei dieser Technik kommen mehrere monoalphabetische Chiffrierungen zum Einsatz.

Beispiel: Vigenère-Code

5.5.7.2 nach der Schlüsselart

a) Symmetrische Verfahren

Bei einem symmetrischen Verschlüsselungsverfahren lässt sich der zum Verschlüsseln benutzte Schlüssel aus demjenigen zum Entschlüsseln berechnen (und umgekehrt). Meistens stimmen die beiden Schlüssel sogar überein (Key1=Key2).

Vorteil: → sehr schnelle Algorithmen
Nachteile: → Ver- und Entschlüsseln mit gleichem Schlüssel
→ Schlüssel muss über einen sicheren Kanal übermittelt werden
→ Sicherheit von Geheimhaltung des Schlüssels abhängig

Beispiele:

1. Cäsar-Verschlüsselung

Beim Verschlüsseln mit dem Cäsar - Code notiert man unter dem Klartextalphabet (KTA) das Geheimtextalphabet (GTA). Das GTA ist im einfachsten Fall eine Verschiebung des KTA um eine bestimmte Anzahl von Stellen.

Sender und Empfänger müssen nur die "Verschiebungszahl" (Schlüssel) vereinbaren. Im folgenden Beispiel wurde das GTA um 4 Stellen gegenüber dem KTA verschoben.

KTA:	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
GTA:	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

Die Verschlüsselung erfolgt nun vom KTA zum GTA. Man sucht den zu verschlüsselnden Buchstaben im KTA und notiert den darunter stehenden Buchstaben des GTA. Beim Entschlüsseln geht man den umgekehrten Weg.

Beispiel:

KTA:	D	A	S	I	S	T	G	E	H	E	I	M
GTA:	H	E	W	M	W	X	K	I	L	I	M	Q

→ Verfahren ist relativ unsicher
→ ein Angreifer müsste max. nur 26 Möglichkeiten probieren, um den Geheimtext zu entschlüsseln
→ Nutzt der Angreifer eine statistische Methode um den Geheimtext zu "knacken", gelangt er schnell ans Ziel, da jeder Buchstabe im Geheimtext (z.B. das E) aus dem gleichen Buchstaben im KTA entstand.

2. Vigenère-Code

Ziel: Häufigkeiten der Buchstaben im Geheimtextalphabet (GTA) möglichst gleich groß zu gestalten

Bei der Verschlüsselung wird nicht nur ein Geheimtextalphabet, sondern verschiedene benutzt; die sich wieder aus der Verschiebung des

Klartextalphabetes (KTA) ergeben. Auf die verschiedenen GTA's wird durch einen festgelegten Schlüssel zugegriffen.

Zunächst notiert man das sogenannte 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

Desweiteren legt man einen Schlüssel selber fest, zum Beispiel:

„I N F O R M A T I K"

Es wird nun der zu verschlüsselnde Text aufgeschrieben und genau darüber das Schlüsselwort so oft notiert, bis das Ende des Textes erreicht ist.

Zum Verschlüsseln des ersten Buchstaben wird in der Zeile, die mit I beginnt, der Buchstabe notiert, der in der Spalte D des KTA's steht. Also das L. Um den zweiten zu verschlüsseln, sucht man den Buchstaben in der Zeile N - Spalte A. Dort findet man das N. Den dritten Geheimbuchstaben findet man in der Zeile F unter der Spalte S. Das ist X.

So ergibt sich z.B. folgender Geheimtext:

Schlüssel:	I	N	F	O	R	M	A	T	I	K	I	N	F	O	R	M	A	T
KTA:	D	A	S	I	S	T	S	T	R	E	N	G	G	E	H	E	I	M
GTA:	L	N	X	W	J	F	S	M	Z	O	V	T	L	S	Y	Q	I	F

Ein Angreifer ist nun nicht mehr in der Lage, zu erkennen, aus welchem Buchstaben sich der Geheimbuchstabe ergab. Die drei „E", die im Klartext vorhanden sind, wurden in verschiedene Buchstaben verschlüsselt. Alle Buchstaben, die im Geheimtext stehen, ergaben sich aus verschiedenen Buchstaben im Klartext.

→ viel sicherer als das einfache Cäsarverfahren
→ Probieren würde nicht zum Erfolg führen
→ statistische Analyse liefert zunächst auch keine Chance
→ erst bei bekannter Länge des Schlüssels kann analytisch

eine Häufigkeit der einzelnen Buchstaben bestimmt werden
→ Sicherheit des Verfahrens steigt mit der Schlüssellänge
→ sicherste Variante wäre bei gleicher Länge von Klartext und Schlüssel

3. Das One Time Pad (OTP)

→ wurde 1917 von Major Joseph Mauborgne und Gilbert Vernam erfunden
→ ist nicht nur praktisch, sondern auch theoretisch unknackbar
→ in der Praxis schwierig umzusetzen, denn:

a) Der Schlüssel muss genauso lang sein wie der Klartext
b) Der Schlüssel muss streng zufällig gewählt sein (keine Pseudo-Zufallszahlen)
c) Der Schlüssel darf nur ein einziges Mal verwendet werden

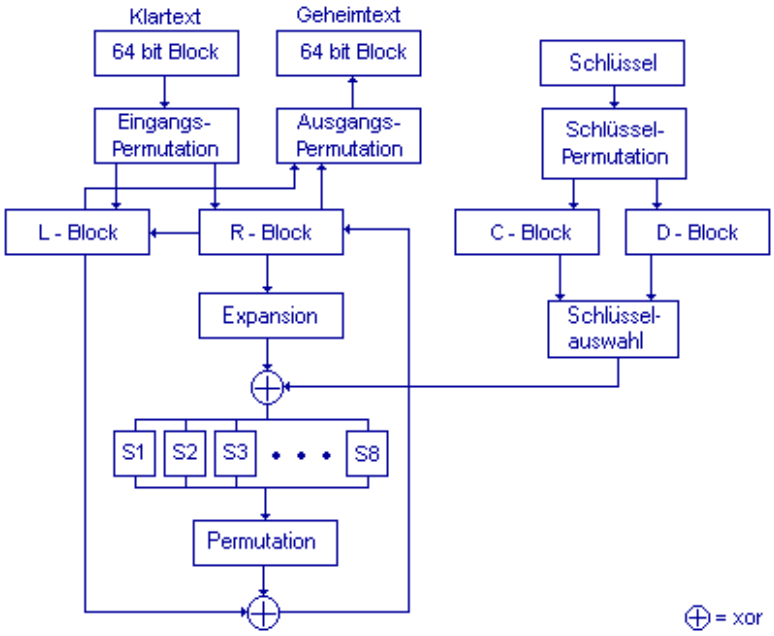
Schlüssel:	1	0	1	0	0	1	1	0	0	1	1	0	1	0
KTA:	0	1	1	0	0	1	0	0	0	1	1	0	0	1
GTA:	1	1	0	0	0	0	1	0	0	0	0	0	1	1

→ Klartext liegt in binärer Form vor
→ der Schlüssel ist eine Zufallsfolge von Bits
→ die Verschlüsselung entsteht, indem die beiden Folgen bitweise durch Exklusiv - Oder (XOR) verknüpft werden
→ die Entschlüsselung erfolgt ebenso durch die XOR – Verknüpfung des Schlüssels und des Geheimtextes.

→ im zweiten Weltkrieg wurde OTP von der englischen Entschlüsselungstruppe von Bletchley Park benutzt, um dem Premierminister die Nachrichten zu übermitteln, die von den Deutschen mit der Enigma verschlüsselt worden waren und die Engländer geknackt hatten.
→ bis vor wenigen Jahren sollen die Gespräche über den "heißen Draht" zwischen dem Weißen Haus und dem Kreml mit Hilfe eines One-Time-Pads verschlüsselt worden sein.

4. DES (Data Encryption Standard)

aus den 64 Bit großen Blöcken des Klartextes erzeugt der DES-Algorithmus 64 Bit große Geheimtexte. Der Schlüssel, der zum Verschlüsseln benutzt wird, hat ebenfalls eine Länge von 64 Bit. Dabei ist jedoch die effektive Schlüssellänge nur 56 Bit, da jedes 8. Bit ein Paritätsbit (dient der Fehlerkontrolle) ist.



→ DES setzt zum Verschlüsseln eine Reihe von Permutationen und Substitutionen ein.

Bemerkungen:
→ wurde 1976 als amerikanischer Standard entwickelt und wird heute am häufigsten eingesetzt.
→ Sicherheit ist bislang sehr hoch, da bis heute noch kein Algorithmus veröffentlicht wurde, der den DES knackt
→ DES ist aber nicht unknackbar (mit leistungsfähigen Rechnern kann man systematisch alle möglichen Schlüssel (2^{56} = ca. 72 Billiarden) probieren; Zeit ca. 22 h)

5. AES (Advanced Encryption)

„Angenommen, ein Super-Computer benötigt 1 Sekunde, um DES zu knacken – so braucht derselbe Super-Computer 149 Tausend-Milliarden Jahre um ein 128 Bit AES zu brechen!“

→ im Oktober 2000 als Nachfolger von DES spezifiziert
→ AES verwendet dabei eine Blockgröße von 128 Bit
→ die Schlüssellänge hat Variabilität von 128, 192 oder 256 Bit beibehalten.
→ durch diese Erhöhung der Schlüssellänge bietet AES ein hohes Maß an Sicherheit

b) Asymmetrische Verfahren

Asymmetrische (oder *Public Key*) Verschlüsselungsverfahren benutzen zwei verschiedene Schlüssel (privater und öffentlicher Schlüssel) zum Ent- und Verschlüsseln, wobei sich der eine nicht aus dem anderen ermitteln lässt.

Privater Schlüssel (private key)

→ muss vom Benutzer sicher verwahrt werden
→ üblicherweise Schutz durch Passwort oder eine Passphrase → dient zum Entschlüsseln von Nachrichten an den Inhaber des privaten Schlüssels

Öffentlicher Schlüssel (public key)

→ ist öffentlich, z. B. auf einem Public Key Server, zugänglich
→ dient zum Verschlüsseln von Nachrichten vom Inhaber des öffentlichen Schlüssels an den Inhaber des privaten Schlüssels (z.B. Senden von Überweisungen an eine Bank)
→ Ein von einer Certification Authority beglaubigter öffentlicher Schlüssel heißt Zertifikat. Ein Zertifikat wird auch als elektronischer Ausweis bezeichnet.

Nachteil: → sehr langsame Algorithmen
Vorteile: → zum Verschlüsseln kann der Schlüssel öffentlich bekannt sein
→ zum Entschlüsseln wird ein, nur dem Eigentümer bekannter, Schlüssel verwendet
→ keine Übertragung von Schlüsseln notwendig

Beispiele:

1. ElGamal-Verfahren

→ 1985 von Taher Elgamal (*Tahir al-Dschamal*) entwickelt
→ beruht Operationen in einer zyklischen Gruppe (höhere Mathematik)

2. RSA-Verfahren

→ 1977 von Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman entwickelt
→ basiert darauf, dass die Faktorisierung einer großen Zahl, also ihre Zerlegung in ihre Primfaktoren, eine sehr aufwändige Angelegenheit ist, während das Erzeugen einer Zahl durch Multiplikation zweier Primzahlen recht einfach ist (Einwegfunktion)
→ aufgrund hoher Rechenleistungen heutiger Computer sollten Schlüssel heute eine Länge von 1024Bit haben
→ Bsp. Kopie

c) Hybride Verfahren

Als hybride Verschlüsselungsverfahren bezeichnet man jene Algorithmen, die symmetrische und asymmetrische Verfahren kombinieren, um die Vorteile der symmetrischen (höhere Geschwindigkeit) und asymmetrischen (Schlüsselaustausch) Verschlüsselungsalgorithmen gleichzeitig nutzen zu können.

Aufgabe:

Anwendung des OTP:

Der Buchstabe A hat den ASCII-Code 65. Dieser kann mit einer 8-stelligen Dualzahl dargestellt werden 01000001.

$0100\ 0001 = 1*2^0 + 0*2^1 + 0*2^2 + 0*2^3 + 0*2^4 + 0*2^5 + 1*2^6 + 0*2^7 = 65$

Die Buchstaben B bis Z entsprechen dem ASCII-Code 66 bis 90.

Welches Wort verbirgt sich hinter:

1100100 0110111 0100111 11011101 GTA
0110001 1110010 1100001 10011100 Schlüssel
KTA