Die Bedeutung von Computersicherheit

- Computersicherheit ist die Sicherheit, die auf Rechengeräte wie Computer und Smartphones sowie auf Computernetzwerke (private und öffentliche) Netzwerke einschließlich des gesamten Internets angewendet wird
- Das Feld umfasst alle Prozesse und Mechanismen, mit denen digitale Geräte, Informationen und Dienste vor unbeabsichtigtem oder unbefugtem Zugriff, Änderung oder Zerstörung geschützt werden
- Das Feld ist von wachsender Bedeutung im Einklang mit der zunehmenden Abhängigkeit von Computersystemen
- Es umfasst physische Sicherheit, um Diebstahl von Geräten zu verhindern, und Informationssicherheit, um die Daten auf diesen Geräten zu schützen. Es wird manchmal als " **cyber security** " oder " **IT security** " bezeichnet

Computersicherheit (Einige wichtige Begriffe)

Verwundbarkeit (vulnerability):

- Verwundbarkeit ist eine Schwachstelle, die es einem Angreifer ermöglicht, die Informationssicherheit eines Systems zu verringern. Die Sicherheitsanfälligkeit ist der Schnittpunkt von drei Elementen:
  - Eine Systemanfälligkeit oder ein Fehler
  - Der Zugriff des Angreifers auf den Fehler
  - Die Fähigkeit des Angreifers, den Fehler auszunutzen
- Um die Sicherheitslücke auszunutzen, muss der Angreifer über mindestens ein geeignetes Tool oder eine geeignete Technik verfügen, mit der eine Verbindung zu einer Systemschwäche hergestellt werden kann
  - In diesem Rahmen wird die Sicherheitslücke auch als **Angriffsfläche** bezeichnet.

Angriffe

- Jeder Vorgang, dessen Folge oder Ziel ein Verlust des Datenschutzes oder der Datensicherheit ist. Auch technisches Versagen wird in diesem Sinne als Angriff gewertet.

- Wenn die Sicherheit eines Systems verletzt wurde, muss es als kompromittiert betrachtet werden, was Maßnahmen zur Verhinderung weiterer Schäden und ggf. zur Datenrettung erfordert.

Klassifizierung nach BSI

- **Schadsoftware bzw. Malware:** ist eine Abkürzung von **Mal**icious Soft**ware**. Einfach gesagt ist Malware eine Software, die mit der Absicht erstellt wurde, Geräte zu beschädigen, Daten zu stehlen oder einfach ein großes Durcheinander zu verursachen. Viren, Trojaner, Spyware gehören zu den verschiedenen Arten von Malware.
- **Ransomware:** eine besondere Form von Schadsoftware, die den Zugriff auf Daten und Systeme einschränkt und dessen Ressourcen erst gegen Zahlung eines Lösegelds wieder freigibt.
- **Social Engineering:** zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen zu bewegen.

Einige wichtige Begriffe

Hintertür (Backdoor):

Eine Hintertür bezieht sich auf jede Methode, mit der autorisierte und nicht autorisierte Benutzer in der Lage sind, normale Sicherheitsmaßnahmen zu umgehen und auf einem Computersystem, in einem Netzwerk oder in einer Softwareanwendung Zugriff zu erhalten. Die Hintertür kann die Form eines installierten Programms (z. B. Back Orifice) haben oder eine Modifikation eines vorhandenen Programms oder eines vorhandenen Hardwaregerätes sein

Einige wichtige Begriffe

Denial-of-service attack :

- Im Gegensatz zu anderen Angriffen werden Denial-of-Service-Angriffe nicht dazu verwendet, unbefugten Zugriff oder Kontrolle über ein System zu erlangen. Sie sind stattdessen so konzipiert, dass sie unbrauchbar werden. Angreifer können einzelnen Opfern den Zugriff verweigern, indem sie beispielsweise absichtlich ein falsches Kennwort so oft eingeben, dass das Konto des Opfers gesperrt wird, oder die Funktionen eines Computers oder Netzwerks überlasten und alle Benutzer gleichzeitig blockieren

- Diese Arten von Angriffen sind in der Praxis sehr schwer zu verhindern, da das Verhalten ganzer Netzwerke analysiert werden muss, nicht nur das Verhalten kleiner Codeteile.

Einige wichtige Begriffe

- Verteilte Denial-of-Service-Angriffe (DDoS) sind häufig, wenn eine große Anzahl kompromittierte Hosts (im Allgemeinen als "Zombie-Computer" bezeichnet) als Teil eines Botnetzes verwendet wird

- Das Botnetz wird verwendet, um ein Zielsystem mit Anfragen zu überfluten und es durch Ressourcenerschöpfung unbrauchbar bzw. unerreichbar zu machen (Availability).

Einige wichtige Begriffe

Abhören (Eavesdropping):

- Abhören ist der Vorgang, bei dem eine private Konversation, normalerweise zwischen Hosts in einem Netzwerk, heimlich abgehört wird. Zum Beispiel wurden Programme wie Carnivore und NarusInsight vom FBI und der NSA verwendet, um die Systeme von Internetdienstanbietern zu belauschen

Einige wichtige Begriffe

Spoofing:

- Das Fälschen der Benutzeridentität beschreibt eine Situation, in der sich eine Person oder ein Programm erfolgreich als eine andere maskiert, indem Daten gefälscht werden und dadurch ein unzulässiger Vorteil erzielt wird.

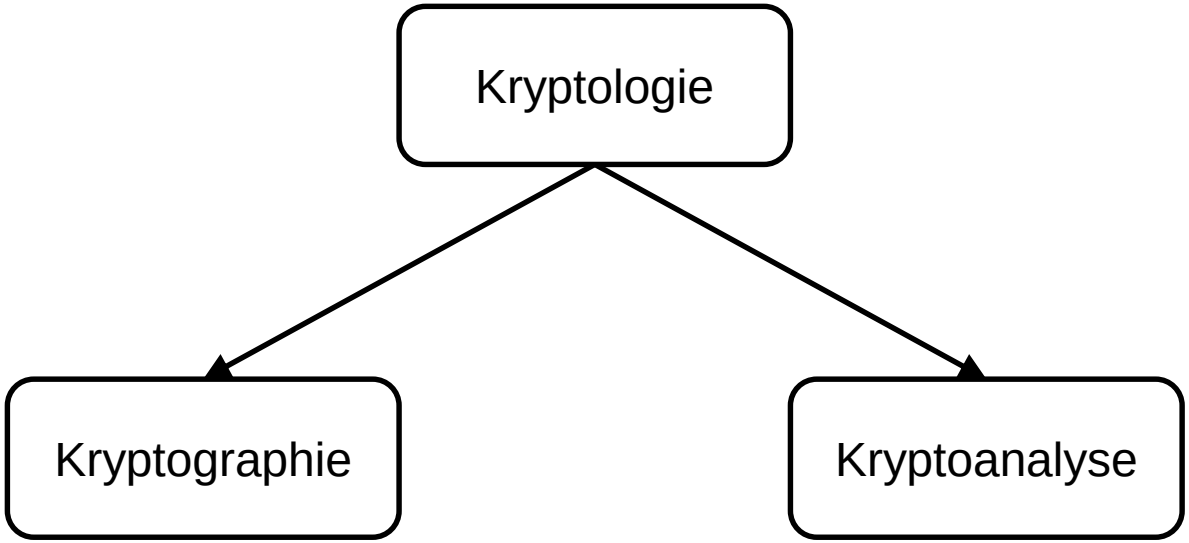
Manipulation (Tampering):

- Unter Manipulation versteht man eine vorsätzliche Veränderung von Produkten, die für den Verbraucher schädlich ist.

Kryptologie

IJNYFhb3Sa9eHNCj7TvlNdwz5db37EmQvot3XYM/83993Uyt5hvv4FnmfDz4eC4h7
nQs3KnOfyajvKGtQlhCTOxk5DkHaPLN8pHtzTZrpNOIWr2AIz/llGCOYhDuXx1lh+I
bDMLio2GXmIwRaPxcjaO+r1Lq4PUaCdLDIOTH8yhoAkxOYZOCXmHmnBlb+gPV
hyesqVsLs2VdMYlz25sNrx/I6uFBSKo9oOVX5h6P7EcFHat2K2q78+EpWGmo7K1
HB6PlxK2Hsjt4ZsmzzQ5sNqQe/WsyZQkbWD2ywHxXJzOlcQDR0qSCZSXkpk79j
VSHDnqAh7cA6cE68UAeZVE2Hq1EfWTKSZkKd3NITOclXPwtvG8TiSSf6eCwdp
SOcMczjq1FaT+GK47s0tl0vtf0FkiGkA09qfq4M91HhNmhHKarJAkp31EH3bYC46d
2Ph6k9xRHUhw/ly5JVMcVWLJyNtyHmDpHEV3LjFNhqSfiDY9kFAlKSVjOSb0eMu
zKyNP8jRR+hk122QFI18qFqp10PnBC6PYBX8u/qj7mei/HBNatXItSQ7aAFGl/aAq
Q1LDUVAK9wIJdawVo6TXuTx81jTunEKI+3mbiBeuNndXeJdoSUevxX1C/DznLHI7
3cRLeFWl3Vwk+vsc+HBBNfYF3ZL2irsm5vWQluaoSwGHLI=

Kryptologie



- Kryptoanalyse: Ein Teilgebiet der Kryptologie neben der Kryptographie. Hier geht es nicht um das Verschlüsseln, sondern über das Entschlüsseln, ohne dass man über den Schlüssel verfügt.

Kryptographie

- Es handelt sich bei der Kryptographie um die Wissenschaft, Methoden, Werkzeuge und Algorithmen zu entwickeln, mit deren Hilfe sich Daten chiffrieren und für Unbefugte unkenntlich machen lassen. Diese sollen den unberechtigtem Zugriff auf Informationen verhindern und einen sicheren Datenaustausch ermöglichen. Nur derjenige, für den die Informationen bestimmt sind, kann die Daten lesen und verarbeiten

- Elementare Ziele sind die **Integrität**, **Authentizität** und **Vertraulichkeit** der Daten. Kryptographie ist auch ein Teilgebiet der Informatik.

Verschlüsselung und Entschlüsselung

Verschlüsselung (Encryption):

- Ist der Vorgang, bei dem eine Nachricht so codiert wird, dass sie für Unbefugte nicht mehr lesbar ist.

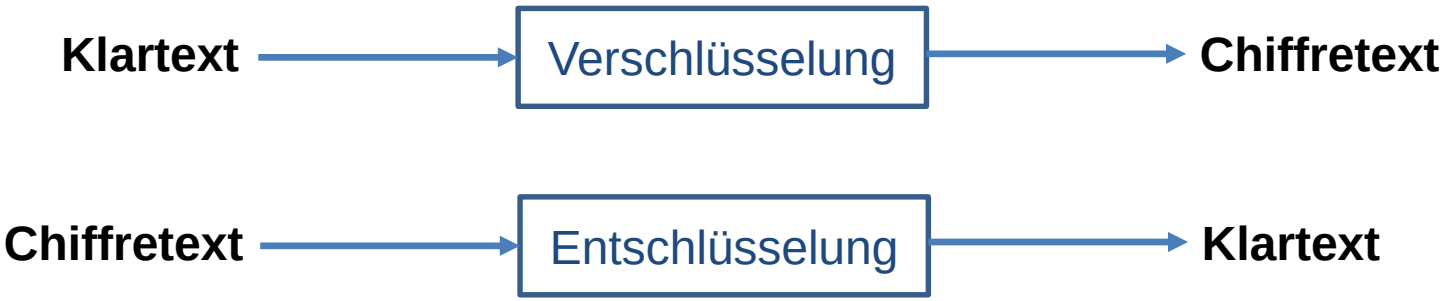
Entschlüsselung (decryption):

- Ist der umgekehrte Vorgang, bei dem eine verschlüsselte Nachricht wieder in die normale umgewandelt wird

Wir sagen, dass wir die ursprüngliche Nachricht verschlüsseln, um ihre Bedeutung zu verbergen. Dann entschlüsseln wir sie, um die ursprüngliche Nachricht zu enthüllen. Ein System zur Ver- und Entschlüsselung wird als **Kryptosystem** bezeichnet.

Verschlüsselung und Entschlüsselung

- Die ursprüngliche Form einer Nachricht wird als **Klartext** bezeichnet, und die verschlüsselte Form wird als **Chiffretext** bezeichnet.
- Der Einfachheit halber bezeichnen wir eine Klartextnachricht mit $\boldsymbol{P}$ als Folge einzelner Zeichen $P = < p1, p2, \ldots, pn >$
- Ebenso wird der Chiffretext als $C = < c1, c2, \ldots, cm >$ geschrieben



Verschlüsselung und Entschlüsselung

- Zum Beispiel die Klartextnachricht „Ich studiere gerne“ kann als Nachrichtenzeichenfolge bezeichnet werden

  $< I, c, h, \ , s, t, u, d, i, e, r, e, \ , g, e, r, n, e >$

- Es kann in Chiffretext umgewandelt werden $< c1, c2, \ldots, c18 >$
- Der Verschlüsselungsalgorithmus sagt uns, wie die Transformation durchgeführt wird
- Wir verwenden diese formale Notation, um die Transformationen zwischen Klartext und Chiffretext zu beschreiben.
  Zum Beispiel:

  Wir schreiben $C = E(P)$ und $P = D(C)$

  E ist die Verschlüsselungsfunktion, D ist die Entschlüsselungsfunktion

$$\boldsymbol{P = D(E(P))}$$

Verschlüsselung und Entschlüsselung

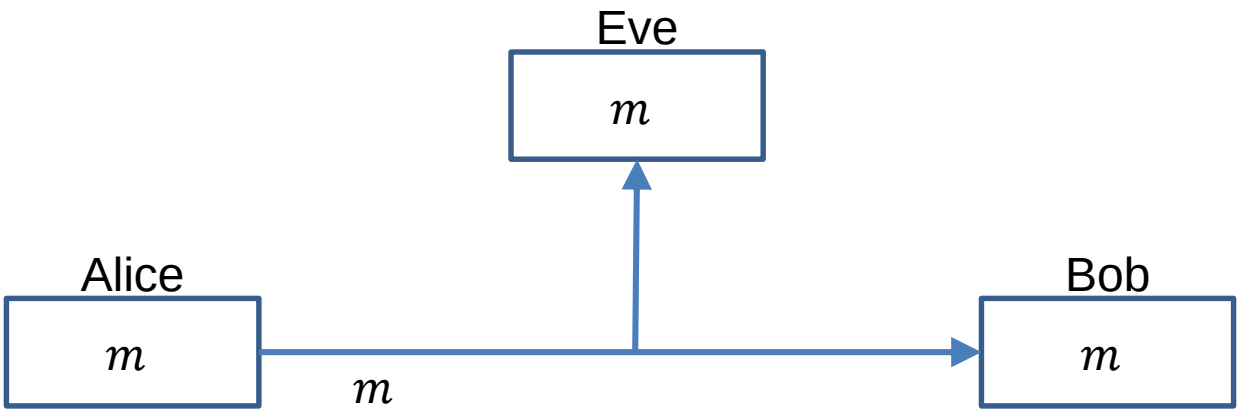
- Mit anderen Worten, wir möchten die Nachricht konvertieren können, um sie vor einem Eindringling zu schützen, aber wir möchten auch die ursprüngliche Nachricht zurückerhalten können, damit der Empfänger sie richtig lesen kann.

- Das Kryptosystem enthält eine Reihe von Regeln zum Verschlüsseln des Klartextes und zum Entschlüsseln des Chiffretextes.

- Die Verschlüsselungs- und Entschlüsselungsfunktionen, die als Algorithmen bezeichnet werden, verwenden häufig einen Schlüssel $\boldsymbol{K}$, sodass der resultierende Chiffretext von der ursprünglichen Klartextnachricht, dem Algorithmus und dem Schlüsselwert abhängt. $C = E(K, P)$

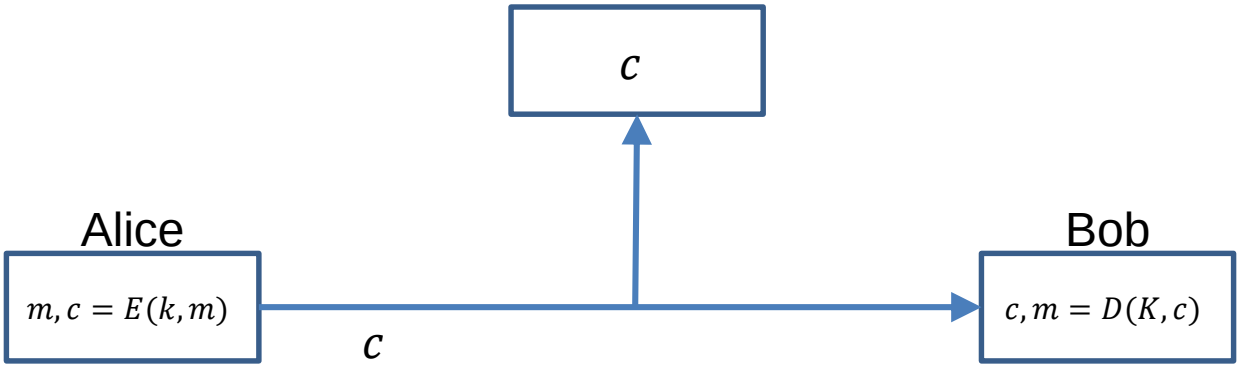
Die generische Einstellung

- Alice und Bob wollen miteinander kommunizieren.
- Eve lauscht auf dem Kanal.
- Jede Nachricht m, die Alice an Bob schickt wird auch von Eve empfangen.
- Wie kann Alice und Bob kommunizieren, ohne dass Eve alles lernt?



Die generische Einstellung

- Um zu verhindern, dass Eve die Nachricht versteht, sie verwenden die Verschlüsselung.
- Alice und Bob vereinbaren zuerst einen geheimen Schlüssel.
- Sie müssen dies über einen Kommunikationskanal tun, auf den Eve nicht lauschen kann.



Kerckhoffs-Prinzip

„Die Sicherheit des Verschlüsselungsschemas darf nur von der Geheimhaltung des Schlüssels und nicht von der Geheimhaltung des Algorithmus abhängen.“

Warum?

- Algorithmen sind schwer zu ändern.
- Sie sind in Software oder Hardware integriert, sie zu ändern ist nicht einfach.
- Niemand baut ein kryptografisches System für nur zwei Benutzer.

Klassische Verfahren

Verschlüsselungsverfahren existieren bereits seit Altertum. Diese frühen Verfahren wurden per Hand ausgeführt. Sie halten der heutigen **Kryptoanalyse** und zur Verfügung stehenden Rechenleistung nicht mehr stand.

- **Substitution:** Bei diesen Verschlüsselungsverfahren werden Zeichen des Klartexte durch andere Zeichen ersetzt.
  - **monoalphabetische Substitution**
  - **polyalphabetische Substitution**

Monoalphabetische Substitution

Bei der monoalphabetischen Substitution kommt lediglich ein einziges Alphabet zum Einsatz. Das heißt, dass jedes Klarzeichen in einem einzelnen, korrespondierenden Geheimtextzeichen resultiert. Wenn z. B. aus einem **A** im Klartext ein **O** im Geheimtext wird, dass ist jedes **O** im Geheimtext ursprünglich ein **A** gewesen.

- **Cäsar Chiffre:** Jeder Klartextbuchstabe wird um eine bestimmte Anzahl von Stellen verschoben. Ist das Alphabet zu Ende, wird wieder von vorne begonnen.
  - Es sind 25 Varianten von dem Verfahren möglich
  - Die 26. Variante würde wieder auf sich selbst abbilden
  - Verschiebung um 13 Zeichen ist ein Sonderfall (ROT-13)

Monoalphabetische Substitution

Mathematisch gesehen: wird jedem Klartextbuchstabenwert (K) die Verschiebung (V) hinzu addiert. Sollte das Ergebnis (C) größer 26 sein, wird 26 abgezogen.

$$C = (K + V)\ mod\ 26$$

Die Entschlüsselung erfolgt entsprechend mit:

$$K = (C - V)\ mod\ 26$$

Monoalphabetische Substitution

Beispiel: Cäsar Chiffre

Klartext: Ichstudieregern, Schlüssel: 3

Übersetzungstabelle Verschiebung 3:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
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

Geheimtext: Lfkvwxglhuhjhuq

Monoalphabetische Substitution

Polybios Chiffre: Das nach dem griechischen Geschichtsschreiber Polybios benannte Verfahren nutzt ein 5x5 (oder 6x6 mit Ziffern) Quadrat, in dass die Buchstaben in der Reihenfolge des Schlüssels niedergeschrieben werden. Als Geheimtext werden dann die Koordinaten der Positionen der Buchstaben notiert und übertragen.

- Normalerweise werden zuerst alle Buchstaben, die im Schlüssel vorkommen, in der Reihenfolge, wie sie im Schlüssel vorkommen, notiert und danach in alphabetischer Reihenfolge der restlichen Buchstaben des Alphabetes.

- Da nur für 25 Buchstaben Platz ist, werden I und J im Klartext gleich behandelt.

Monoalphabetische Substitution

Beispiel: Polybios Chiffre

Klartext: Ichstudieregern, Schlüssel: Infosec

	1	**2**	**3**	**4**	**5**
1	I	N	F	O	S
2	E	C	A	B	D
3	G	H	K	L	M
4	P	Q	R	T	U
5	V	W	X	Y	Z

Geheimtext: 11 22 32 15 44 45 25 11 21 43 21 31 21 43 12

Monoalphabetische Substitution

Playfair Chiffre: Der Chiffre liegt ein Polybios-Quadrat zugrunde, dass wie üblich aus dem Schlüsselwort erstellt wird.

- Dann gruppiert man die Buchstaben des Klartextes in Zweier-Pärchen
- Da Buchstaben-Pärchen mit demselben Buchstaben ein Problem für den Algorithmus darstellen, wird zwischen sie ein 'X' eingeschoben.
- Ggf. wird das letzte Pärchen mit einem A aufgefüllt

Monoalphabetische Substitution

Je Pärchen werden dann folgende Bedingungen bzgl. des Quadrates abgefragt:

1. **Beide Buchstaben befinden sich in derselben Zeile**: Es werden die jeweils nachfolgenden Buchstaben (rechts vom Original) genommen. Ist es der letzte Buchstabe der Zeile, wird der erste Buchstabe in der Zeile genommen.
2. **Beide Buchstaben befinden sich in derselben Spalte**: Es werden die jeweils darunter befindlichen Buchstaben (unter dem Original) genommen. Ist es der letzte Buchstabe der Spalte, wird der erste Buchstabe in der Spalte genommen.
3. **Keine der beiden oberen Bedingungen trifft zu**: Wird ein Rechteck mit den beiden Originalbuchstaben als Eckpunkte gebildet und die beiden entstehenden Eckpunkte genommen (zuerst in der Zeile des 1. Buchstabens, dann in der Zeile des 2. Buchstabens).

Monoalphabetische Substitution

Beispiel: Playfair Chiffre

Klartext: Ichstudieregern, Schlüssel: Infosec

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

Bildung der Zweier-Pärchen: Ic hs tu di er eg er na

Ic → NE = Regel 3
hs → MN = Regel 3
Tu → UP = Regel 1

Geheimtext: NEMNUPESAPGPAPFW

Monoalphabetische Substitution

Four-Square Chiffre: Die Four-Square Chiffre wurde von dem Franzosen Felix Delastelle entwickelt und ist eine Art Polybios-Chiffre mit 2 Alphabeten und 2 Schlüssel-Quadraten, also insgesamt 4 Quadraten, daher auch der Name.

- vier Quadrate in einer 2x2 Matrix niedergeschrieben
- die Quadrate oben links und unten rechts enthalten das normale Alphabet (außer J)
- Das Quadrat oben rechts enthält ein 5x5 Polybios Quadrat des 1. Schlüssels
- Das Quadrat unten links enthält ein 5x5 Polybios Quadrat des 2. Schlüssels

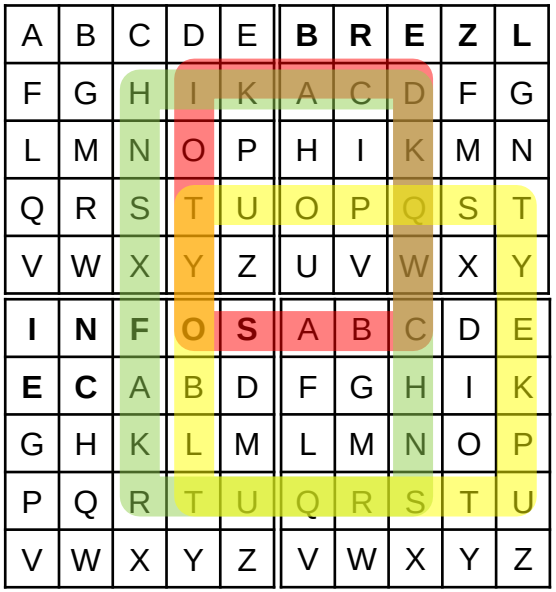
Monoalphabetische Substitution

- Dann gruppiert man die Buchstaben des Klartextes in Zweier-Pärchen
- Ggf. wird das letzte Pärchen mit einem X aufgefüllt
- Je Pärchen markiert man nun die zwei Buchstaben in den Klartext-Quadrate (1. Buchstaben oben links, 2. unten rechts)
- Man denkt sich ein Rechteck, dass diese beiden Buchstaben miteinander verbinden würden. Die beiden 'Ecken' werden als Geheimtext aufgeschrieben: zuerst den Buchstaben des Quadrats oben rechts (1. Schlüsselwort), dann den Buchstaben des Quadrates unten links (2. Schlüsselwort).

Monoalphabetische Substitution

Beispiel: Four-Square Chiffre

Klartext: Ichstudieregern, Schlüssel 1: Brezel, Schlüssel 2: Infosec



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

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

Bildung der Zweier-Pärchen: Ic hs tu di er eg er nx

Ic → DO
hs → DR
Tu → TT
Geheimtext: DODRTTZBRURDRUKX

Polyalphabetische Substitution

- Im Gegensatz zur monoalphabetischen Substitution werden für zur Erzeugung des Geheimtextes aus dem Klartext viele Geheimalphabete verwendet.
- So wird bspw. das 1. Zeichen des Klartextes mit dem 1. Schlüsselalphabet verschlüsselt, das 2. Zeichen mit dem 2. Schlüsselalphabet.
- Das Problem der monoalphabetischen Substitution, dass man durch Häufigkeitsanalysen der Zeichen des Geheimtextes mit etwas Probieren oft auf den Klartext zurückgeschlossen werden kann, wird dadurch verhindert, weil ja nur jeder **n-te** Buchstabe zu einem Schlüsselalphabet gehört.
- Wobei n die Anzahl der Schlüsselalphabete ist, die einem Angreifer zu Beginn unbekannt ist.

Polyalphabetische Substitution

Der Nachteil der polyalphabetischen Substitution ist, dass jedes Schlüsselalphabet auch ein eigens Schlüssel bedarf und man sich diese Schlüssel auch merken bzw. diese transportieren muss.

- **Nihilisten Substitution :**
  - Dem Chiffre liegt ein Polybios-Quadrat zugrunde, dass wie üblich aus dem Schlüsselwort erstellt wird.
  - Zuerst wird der Klartext via Polybios mit dem 1. Schlüsselwort verschlüsselt.
  - Danach wird das 2. Schlüsselwort mit ddem 1. Schlüsselwort verschlüsselt

Polyalphabetische Substitution

- Die einzelnen Summen werden nun addiert und ergeben Werte von 22 bis 110, die das Geheimtext darstellen.

- Dabei werden von Werten über 99 die führende „1“ ignoriert, um zweistellig zu bleiben.

- Bei Dechiffrieren werden dann allen Werten unter 22 wieder 100 aufaddiert.

- Um den Geheimtext wieder zu entschlüsseln muss jetzt einfach nur das Passwort, vom Geheimtext abgezogen werden.

- Nun kann man die Matrix zur Entschlüsselung nutzen, indem den Ziffern ihre jeweiligen Buchstaben zugeordnet werden.

Polyalphabetische Substitution

	1	**2**	**3**	**4**	**5**
1	I	N	F	O	S
2	E	C	A	B	D
3	G	H	K	L	M
4	P	Q	R	T	U
5	V	W	X	Y	Z

5 * 5 Matrix mit dem Schlüssel 1.

Klartext: Ichstudieregern
Schlüssel 1: Infosec, Schlüssel 2: Brezel

I	C	H	S	T	U	D	I	E	R	E	G	E	R	N
11	22	32	15	44	45	25	11	21	43	21	31	21	43	12

Klartext verschl. mit dem Schlüssel 1

B	R	E	Z	E	L	B	R	E	Z	E	L	B	R	E
24	43	21	55	21	34	24	43	21	55	21	34	24	43	12

Schlüssel 2 verschl. mit dem Schlüssel 1

Polyalphabetische Substitution

I	C	H	S	T	U	D	I	E	R	E	G	E	R	N
11	22	32	15	44	45	25	11	21	43	21	31	21	43	12

Klartext verschl. mit dem Schlüssel 1

B	R	E	Z	E	L	B	R	E	Z	E	L	B	R	E
24	43	21	55	21	34	24	43	21	55	21	34	24	43	12

Schlüssel 2 verschl. mit dem Schlüssel 1

11	22	32	15	44	45	25	11	21	43	21	31	21	43	12
24	43	21	55	21	34	24	43	21	55	21	34	24	43	12
35	65	53	70	65	79	49	54	42	98	42	65	45	86	24

Geheimtext: 35 65 53 70 65 79 49 54 42 98 42 65 45 86 24

Polyalphabetische Substitution

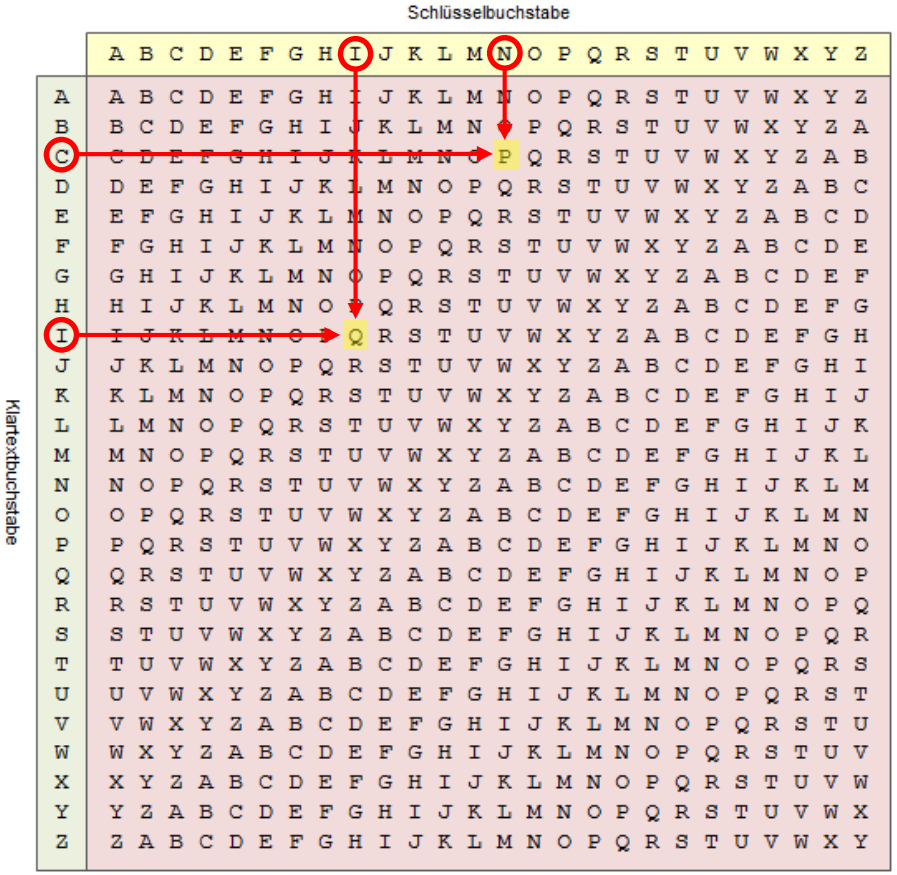
Vigenere Chiffre:

- Galt lange als sicherer Chiffrieralgorithmus.
- Eine Übersetzungstabelle, das sogenannte Vigenere-Quadrat wird benutzt.
- Ist der Schlüssel verbraucht, wird bei Beginn des Schlüssels weiter verarbeitet.
- Wir suchen den Klartextbuchstaben links in der 1. Spalte und gehen in dieser Zeile soweit nach rechts, bis wir in der obersten Zeile den Buchstaben des Schlüssels gefunden haben.
- Nun können wir dort den Chiffre-Buchstaben ablesen.

Polyalphabetische Substitution

- Wir können auch ohne Übersetzungstabelle verschlüsseln (Mathematisch) .
- Dafür verwenden wir die Offsets, die sich aus dem Schlüssel ergeben.
- Dabei hat A den Wert 0, B den Wert 1 usw.
- Der Offset wird dem Klartextbuchstaben dann hinzuaddiert, um den Chiffratbuchstaben zu erhalten.

Polyalphabetische Substitution



Klartextbuchstabe	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

Klartext: Ichstudieregern
Schlüssel: Infosec

I → Q
c → p

Geheimtext: Qpmglyfqrwsyitv

Polyalphabetische Substitution

Mathematisch: Klartext: Ichstudieregern, Schlüssel: Infosec

- Schlüssellänge = 7.

1, 2, 3 * Schlüssellänge datzu addieren

							1							2							3					Offset
0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	
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	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	

I	C	H	S	T	U	D	I	E	R	E	G	E	R	N
I	N	F	O	S	E	C	I	N	F	O	S	E	C	I
+8	+13	+5	+14	+18	+4	+2	+8	+13	+5	+14	+18	+4	+2	+8
Q	p	m	g	l	y	f	q	r	w	s	y	i	t	v

Transposition

- Im Gegensatz zur Substitution werden hier die Zeichen nicht ersetzt, sondern untereinander vertauscht.
- Die Anzahl und Häufigkeit der Zeichen bleibt also gleich, nur deren Position im Geheimtext ändert sich.
- Dies steht im Gegensatz zu monoalphabetischen bzw. polyalphabetischen Subsitutionschiffren wo der Klartext durch andere Zeichen ersetzt wird.

Transposition

Gartenzaun:

- Wird auch Zick-Zack genannt.

- Die Buchstaben des Klartextes werden abwechselnd in mehrere (Tiefe bzw. Schlüssel) Zeilen geschrieben, so dass ein Zickzack-Muster entsteht.
- Danach wird der Text Zeile für Zeile ausgelesen und die Leerzeichen dazwischen ignoriert.
- Die Tiefe muss bei der Verschlüsselung angegeben werden.

Transposition

Klartext: Ichstudieregern, Schlüssel: 3

I		t		e		e
	c		s		u	
		h		d		e
			i		r	
				r		n
					g	

Zeilenweise auslesen (Geheimtext): Iteecsuirgrhden

- Man kann einfach alle Tiefen, die in Frage kommen nacheinander durchprobieren und muss dann nur noch den Klartext bei der richtigen Tiefe (entspricht dem Schlüssel) erkennen.

Transposition

Gartenzaun mit einem zweiten Passwort (*Redefence Cipher***)**:

Klartext: Ichstudieregern, Schlüssel: 3, ISO

I	t	e	e	1
c	s	u	i	r	g	r	2
h	d	e	n	3

I	S	O
1	3	2

Zeilenweise in der Reihenfolge des Passwortes auslesen

(Geheimtext): Iteehdencsuirgr

Transposition

Doppelwürfel:

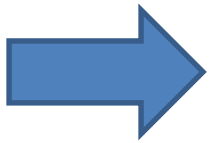
- Zwei Schlüssel werden benötigt.
- Der Klartext wird zeilenweise in ein Rechteck (Matrix) eingetragen, dessen Breite von der Länge des angewendeten Schlüssels bestimmt wird.
- Die Spaltenanzahl entspricht also der Anzahl der Buchstaben dieses Schlüsselworts
- Die Höhe des Würfels (also die vertikale Seitenlänge) ist abhängig von der Länge des verwendeten Textes.

Transposition

Beispiel: Doppelwürfel

Klartext: Ichstudieregernauchwennesnichtimmereinfachist,
Schlüssel 1: Infosec, Schlüssel 2: Brezel

I	N	F	O	S	E	C
4	5	3	6	7	2	1
I	C	H	S	T	U	D
I	E	R	E	G	E	R
N	A	U	C	H	W	E
N	N	E	S	N	I	C
H	T	I	M	M	E	R
E	I	N	F	A	C	H
I	S	T				



C	E	F	I	N	O	S
1	2	3	4	5	6	7
D	U	H	I	C	S	T
R	E	R	I	E	E	G
E	W	U	N	A	C	H
C	I	E	N	N	S	N
R	E	I	H	T	M	M
H	C	N	E	I	F	A
		T	I	S		

Transposition

- Wie zu sehen, ist die letzte Zeile nicht vollständig gefüllt.
- Dies ist nur dann der Fall, wenn die Schlüssellänge ein ganzzahliger Teiler der Klartextlänge ist.
- Wie zu erkennen, hat sich die Position der Lücken wegen Sortierung verändert - dies kann allerdings ignoriert werden.
- Der nächste Schritt, ist das spaltenweise Auslesen der entstandenen Matrix.
- Das Ergebnis wird also nicht in Lesereihenfolge entnommen, sondern spaltenweise.
- Zusammenfassend wurden der Klartext eingetragen, die Spalten in Abhängigkeit eines Schlüssels vertauscht und das Ergebis spaltenweise ausgelesen.

Transposition

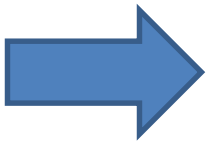
Geheimtext der ersten Runde: **DRECR HUEWI ECHRU EINTI INNHE ICEAN TISSE CSMFT GHNMA**

- Um die Sicherheit der Chiffre zu verstärken, muss dieser Vorgang - unter Verwendung eines zweiten unabhängigen Schlüssels - erneut durchgeführt werden.
- In diesem Beispiel verwenden wird den Schlüssel Brezel und es ergibt sich ein neues Rechteck der Breite 6.
- Der Klartext der zweiten Runde, ist der Chiffretext der ersten und dieser wird zeilenweise in den Würfel eingetragen.
- Anschließend wird erneut die Spaltentransposition durchgeführt, wie sie bereits für die vorherige Runde beschrieben wurde.

Transposition

Beispiel: Doppelwürfel
Klartext (Geheimtext der ersten Runde):
DRECRHUEWIECHRUEINTIINNHEICEANTISSECSMFTGHNMA, Schlüssel 2: Brezel

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			



B	E	E	L	R	Z
1	2	3	4	5	6
D	E	R	H	R	C
U	W	E	C	E	I
H	U	I	N	R	E
T	I	N	H	I	N
E	C	A	N	I	E
T	S	E	C	I	S
S	F	G	H	M	T
N	A			M	

Transposition

- Nachdem der Würfel spaltenweise permutiert wurde, kann man das Ergebnis der zweiten Runde auslesen.

- Wie zuvor wird erneut spaltenweise vorgegangen, um den resultierenden Chiffretext zu gewinnen.

Geheimtext:

DUHTETSNEWUICSFAREINAEGHCNHNCHRERIIIMMCIENEST

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

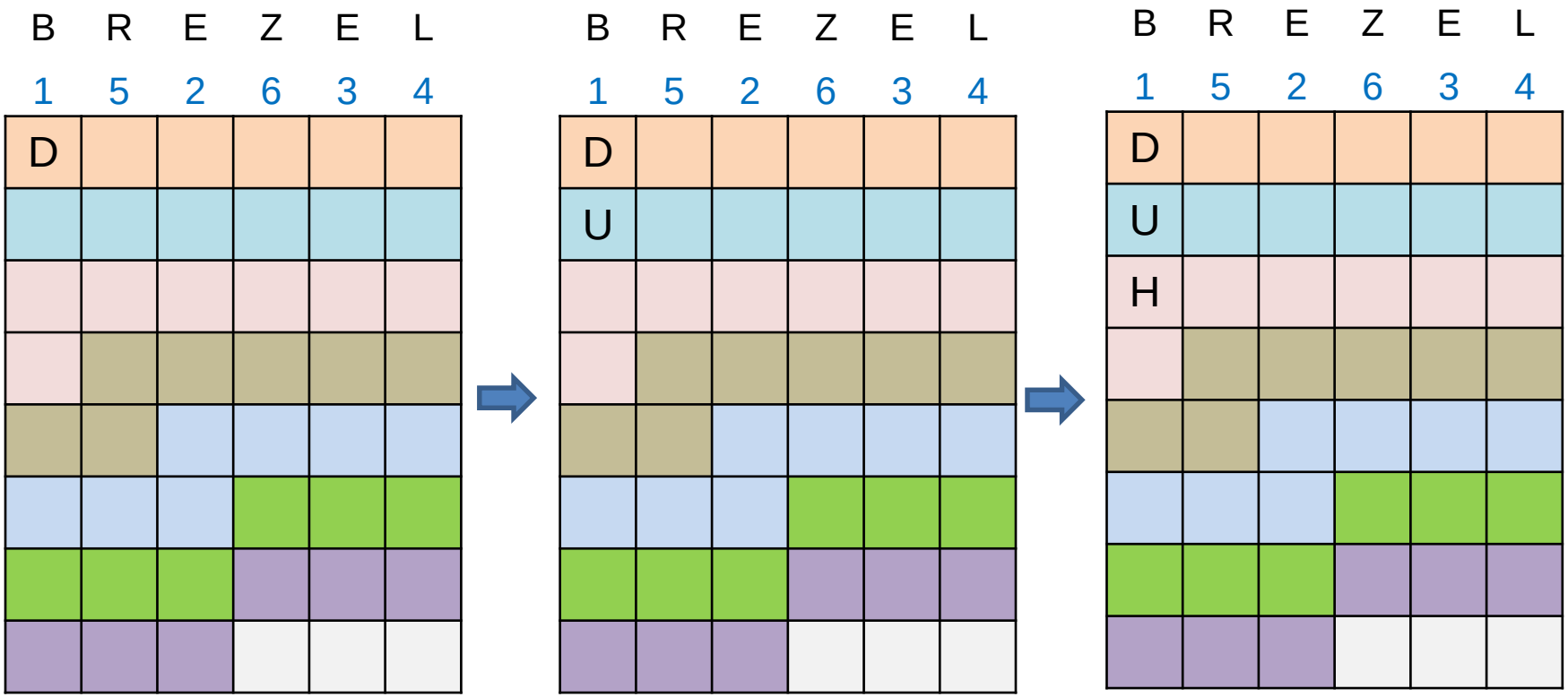
- Die Schritte der Verschlüsselung werden rückwärts ausgeführt.
- Zunächst wird ein leerer Würfel der zweiten Runde aufgestellt.

B	R	E	Z	E	L
1	5	2	6	3	4

- Nun kann der Chiffretext spaltenweise in die Matrix eingetragen werden.
- Die Reihenfolge der Eintragung entspricht der Reihenfolge der Schlüsselzeichen im Alphabet.
- Das Entschlüsselungsergebnis der ersten Runde ist das zeilenweise Auslesen des entstandenen Würfels.

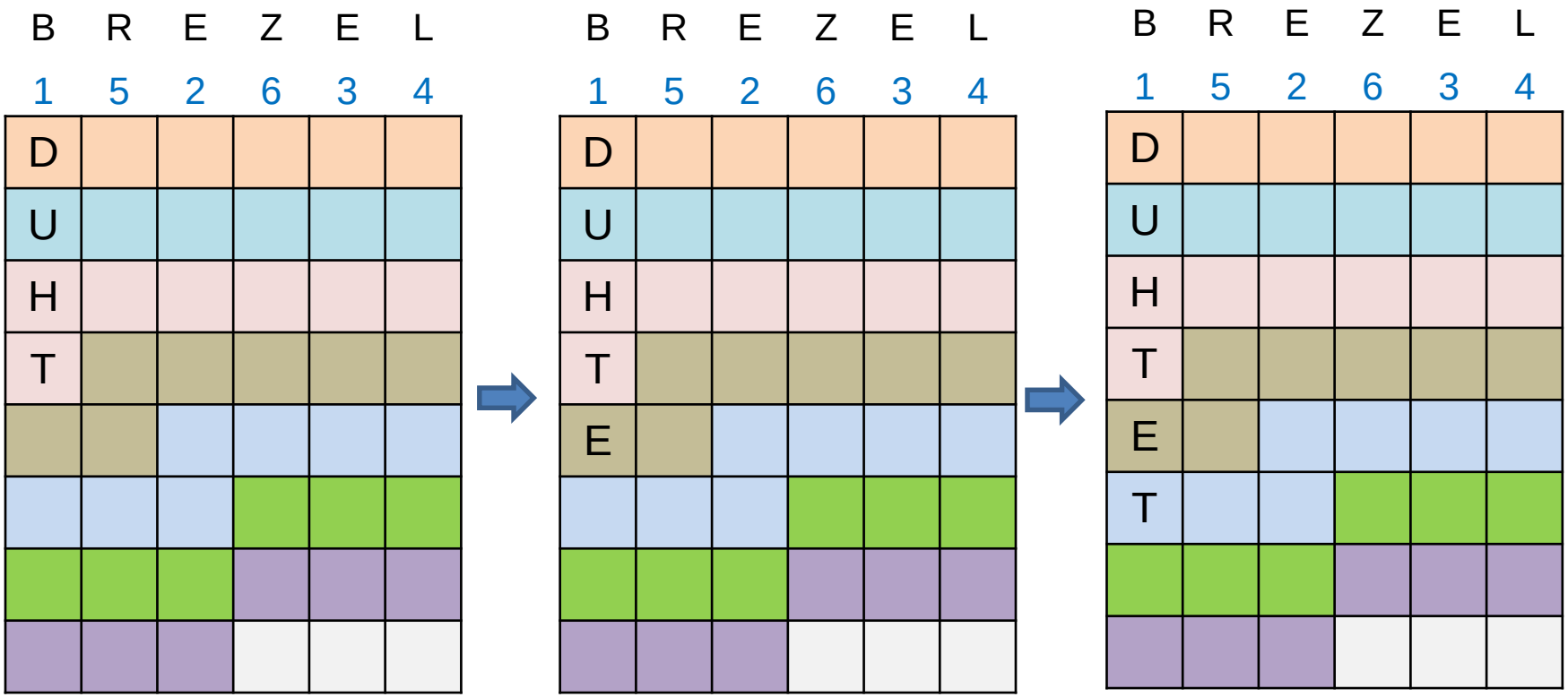
Transposition

Beispiel: Doppelwürfel (Entschlüsselung)
Geheimtext:
DUHTETSNEWUICSFAREINAEGHCNHNCHRERIIIMMCIENEST



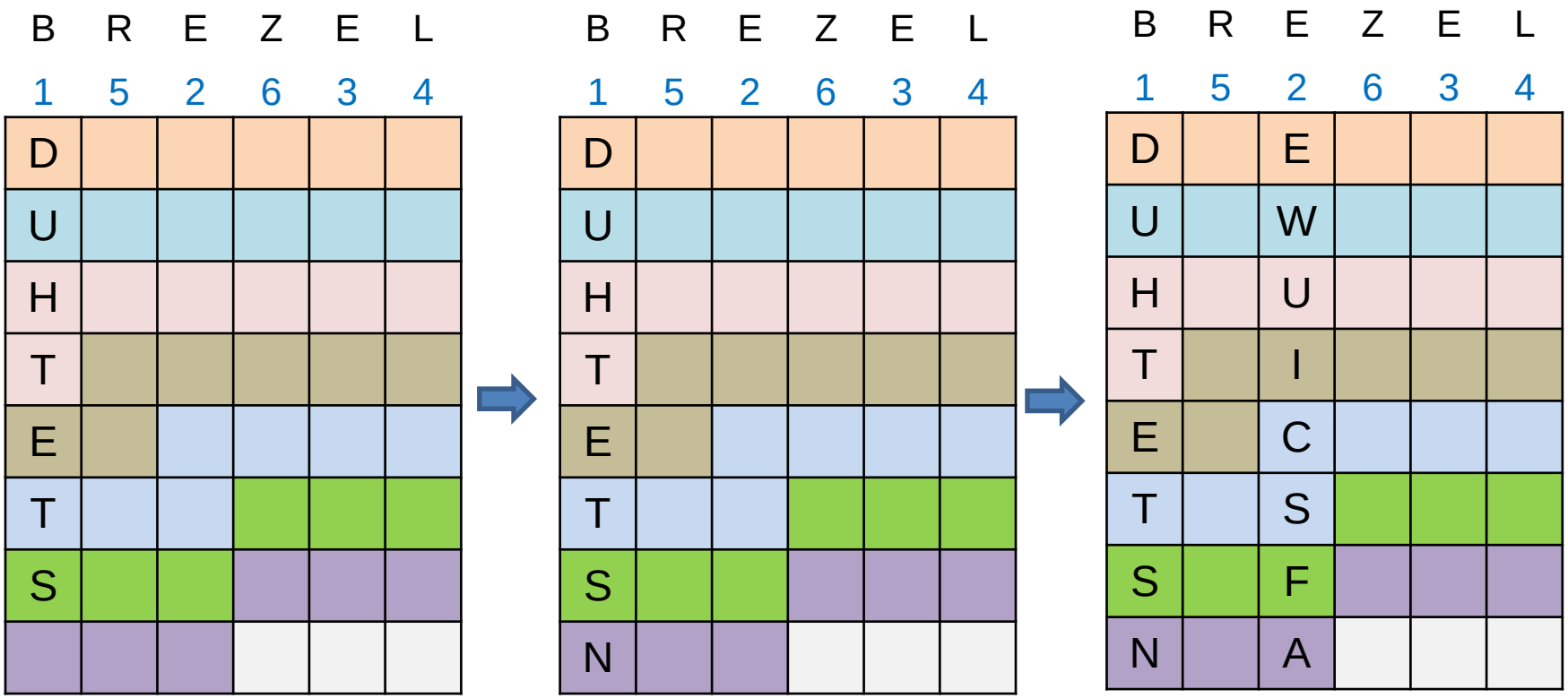
Transposition

Beispiel: Doppelwürfel (Entschlüsselung)
Geheimtext:
DUHTETSNEWUICSFAREINAEGHCNHNCHRERIIIMMCIENEST



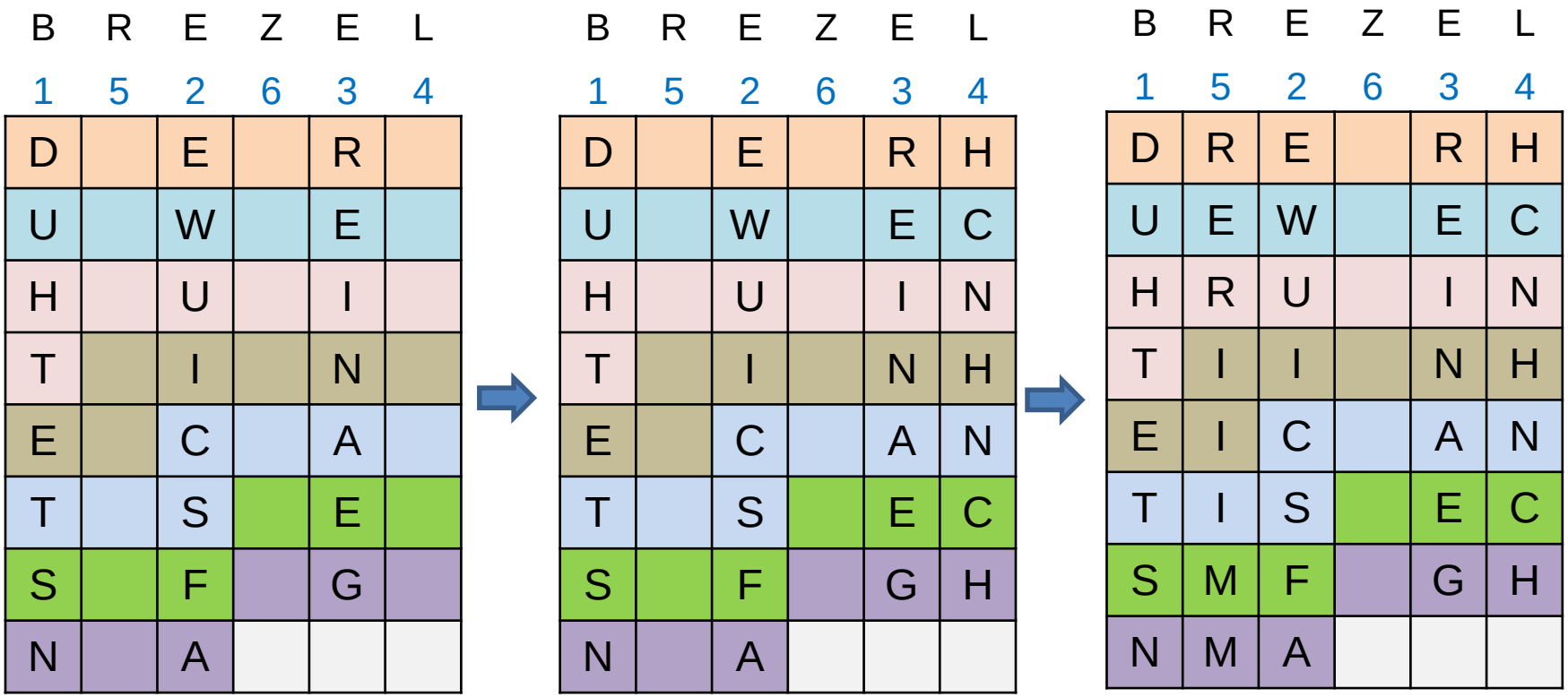
Transposition

Beispiel: Doppelwürfel (Entschlüsselung)
Geheimtext:
DUHTETSNEWUICSFAREINAEGHCNHNCHRERIIIMMCIENEST



Transposition

Beispiel: Doppelwürfel (Entschlüsselung)
Geheimtext:
DUHTETSNEWUICSFAREINAEGHCNHNCHRERIIIMMCIENEST



Transposition

Beispiel: Doppelwürfel (Entschlüsselung)
Geheimtext:
DUHTETSNEWUICSFAREINAEGHCNHNCHRERIIIMMCIENEST

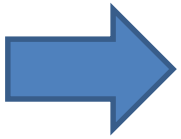
B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			

- Analog kann dieser Vorgang für die zweite Entschlüsselungsrunde mit dem ersten Schlüssel der Verschlüsselung durchgeführt werden.
- Wichtig ist hierbei erneut, dass die Spalten mit Überlänge bzw. die Spalten mit fehlenden Feldern in der letzten Zeile beachtet werden.
- Als Resultat kann der Klartext nun wieder zeilenweise aus dem Würfel entnommen und gelesen werden.

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			

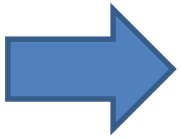


I	N	F	O	S	E	C
4	5	3	6	7	2	1

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			

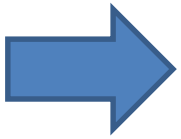


I	N	F	O	S	E	C
4	5	3	6	7	2	1
						D
						R
						E
						C
						R
						H

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			

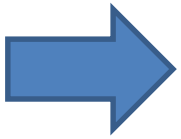


I	N	F	O	S	E	C
4	5	3	6	7	2	1
					U	D
					E	R
					W	E
					I	C
					E	R
					C	H

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			

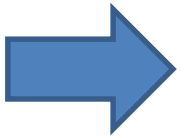


I	N	F	O	S	E	C
4	5	3	6	7	2	1
		H			U	D
		R			E	R
		U			W	E
		E			I	C
		I			E	R
		N			C	H
		T				

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			

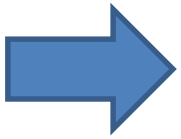


I	N	F	O	S	E	C
4	5	3	6	7	2	1
I		H			U	D
I		R			E	R
N		U			W	E
N		E			I	C
H		I			E	R
E		N			C	H
I		T				

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			

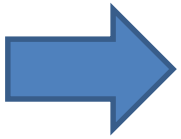


I	N	F	O	S	E	C
4	5	3	6	7	2	1
I	C	H			U	D
I	E	R			E	R
N	A	U			W	E
N	N	E			I	C
H	T	I			E	R
E	I	N			C	H
I	S	T				

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			



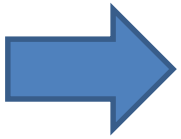
I	N	F	O	S	E	C
4	5	3	6	7	2	1
I	C	H	S		U	D
I	E	R	E		E	R
N	A	U	C		W	E
N	N	E	S		I	C
H	T	I	M		E	R
E	I	N	F		C	H
I	S	T				

Transposition

Beispiel: Doppelwürfel (Entschlüsselung)

Klartext: Ichstudieregernauchwennesnichtimmereinfachist

B	R	E	Z	E	L
1	5	2	6	3	4
D	R	E	C	R	H
U	E	W	I	E	C
H	R	U	E	I	N
T	I	I	N	N	H
E	I	C	E	A	N
T	I	S	S	E	C
S	M	F	T	G	H
N	M	A			



I	N	F	O	S	E	C
4	5	3	6	7	2	1
I	C	H	S	T	U	D
I	E	R	E	G	E	R
N	A	U	C	H	W	E
N	N	E	S	N	I	C
H	T	I	M	M	E	R
E	I	N	F	A	C	H
I	S	T				