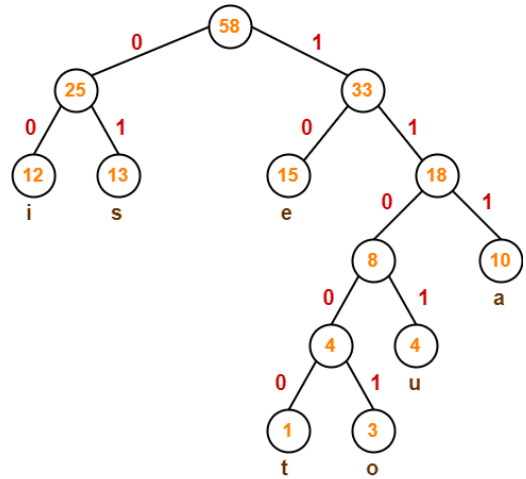


Huffman:

Alle Buchstaben aufteilen, Buchstaben zählen. (Häufigkeitsanalyse)
Wenigsten nach unten und meisten nach oben. (Baum erstellen)
!!! Möglichst ähnliche Häufigkeit in einer Zeile !!!



LZ77:

Puffer, Vorschau Fenster, Code
Erster Buchstaben in Vorschau Fenster encoden.
In den Puffer schieben, Code schreiben
Codeaufbau: (Stelle im Puffer, Anzahl Buchstaben im Puffer, neuster encodeter Buchstaben)

Puffer							Vorschau Fenster			Code
1	2	3	4	5	6	7	↓			
							B	A	N	A (0,0,B)
						B	A	N	A	N (0,0,A)
				B	A	N	A	N	E	(0,0,N)
		B	A	N			A	N	E	(6,2,E)
B	A	N	A	N	E					(-, -, -)

(0,0,B)(0,0,A)(0,0,N)(6,2,E),(-,-,-)

Huffman Tree

Rekonstruktion:

1	2	3	4	5	6	7	
							B (0,0,B)
						B	A (0,0,A)
						B A	N (0,0,N)
						B A N	E (6,2,E)
						B A N A N E	(-, -, -)

LZ78:

Wörterbuch mit allen enthaltenen Buchstaben erstellen.
Anfang: in letztes Wort nichts eintragen, aktuelles Wort = erster Buchstabe.
LW + AW im Wörterbuch -> kein Eintrag/Code
LW + AW nicht im Wörterbuch -> Eintrag/Code erstellen

Wörterbuch	letztes Wort	aktuelles Wort	WB-Eintrag	Code
B = 1		B		
A = 2	B	A	BA=7	1
U = 3	A	U	AU=8	2
M = 4	U	M	UM=9	3
S = 5	M	S	MS=10	4
R = 6	S	A	SA=11	5
BA = 7	A	U		
AU = 8	AU	M	AUM=12	8
UM = 9	M	R	MR=13	4
MS = 10	R	A	RA=14	6
SA = 11	A	U		
AUM = 12	AU	M		
MR = 13	AUM	-		12
RA = 14				

BWT (Burrow-Wheeler-Transformation):

-> Keine Komprimierung, sondern Vorbereitung für RLE
RLE = Run Length Encoding

An Schluss von Wort Dollar Zeichen anhängen.
In erste Zeile einsetzen, jede weitere Zeile eins nach links verschieben,
bis Dollar Zeichen am Anfang.

Nach Alphabet sortieren -> letzte Spalte sortiert
In RLE umschreiben (Buchstabe und danach Anzahl, einzelner Buchstabe keine Anzahl)

Decoding:

Linkes Dollar anfangen, gerade nach rechts -> erster Buchstabe
In linker Spalte nach gleichem Buchstaben suchen. gerade nach rechts -> zweiter Buchstabe, ...

✓	A	N	A	N	A	S	\$
✓	N	A	N	A	S	\$	A
✓	A	N	A	S	\$	A	N
✓	N	A	S	\$	A	N	A
✓	A	S	\$	A	N	A	N
✓	S	\$	A	N	A	N	A
✓	\$	A	N	A	N	A	S



\$	A	N	A	N	A	S	\$
A	N	A	N	A	S	\$	A
A	N	A	S	\$	A	N	A
A	S	\$	A	N	A	N	A
N	A	N	A	S	\$	A	N
N	A	S	\$	A	N	A	A
S	\$	A	N	A	N	A	A

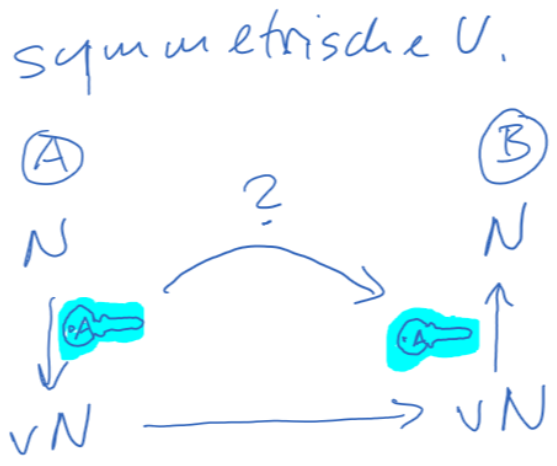
↓ S \$ N N A A A = S \$ N 2 A 3
BWT RLE



A₁N₁A₂N₂A₃S\$

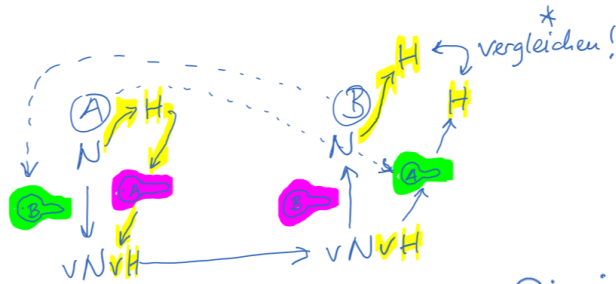
Sym. / Asym. Verschlüsselung (Hybride):

Sym. V.:
A verschlüsselt mit Key -> B entschlüsselt mit Key
Asym. V.:
A verschlüsselt mit public Key von B -> B entschlüsselt mit Private Key von B
Nachteile: hohe Rechenleistung, nur in eine Richtung verschlüsselt
Hybride V.:
Schlüsseltausch -> asym.
Kommunikation -> sym.



Hash:

Hash aus Nachricht, Hash mit Schlüssel verschlüsselt,
Verschlüsselte Nachricht kann mit Schlüssel zum Hash gemacht werden,
aus Hash wird Nachricht gemacht.



Historische Versch.:

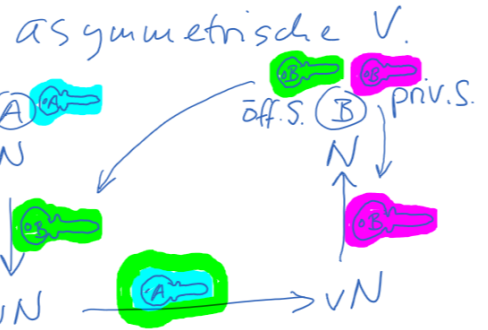
-- Caesar --
Buchstaben verschieben,
z.B. hallo +2 -> jcnqg

-- Vigenère --
variable Versch.
durch "Passwort"

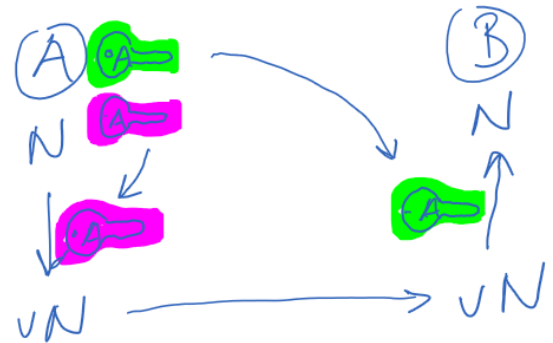
Bsp hallo, Passwort "ja"

h	a	l	l	o
8	1	12	12	15
10	1	10	1	10
<hr/>				
18	2	22	13	25
r	b	v	m	y

* Wenn gleiche Hashes
-> Unterschrift OK!
-> Nachricht nicht verändert!



Digitale Unterschrift



-- Vernam --

Gleich Vigenère, Passwort gleich lang wie Nachricht

SSL-Zertifikat = Datei

- Eigentümer B
- Ablaufdatum
- Zertifizierungsstelle
- CRL = Certificate Revocation List = Rückmelde-Liste -> LDAP-Server

AES

1. Substitution: Ersetzen der Zellen gemäß S-Box
2. Shift Row: Verschieben der Zeilen um bestimmten Wert
3. Mix Column: Multiplikation mit Matrix
4. Key Addition: XOR-Verknüpfung von Matrix mit runden Schlüssel

Abkürzungen

	früher	heute
symm.	DES Data Encryption Standard	AES AES-128 AES-192 AES-256 Advanced Encryption Standard
asymm.	DH Diffie-Hellman	RSA Rivest-Shamir-Adleman
hybrid	SSL Secure Sockets Layer	TLS Transport Layer Security
Hash		SHA Secure Hash Algorithm
Email		PGP (Open PGP) Pretty Good Privacy S/MIME Secure Multipurpose Internet Mail Extensions