



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Kryptographie

Prof. Dr. Björn Grohmann

THE QUEEN OF SCOTS



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Maria Stuart

8. Dezember 1542 -- 8. Februar 1587

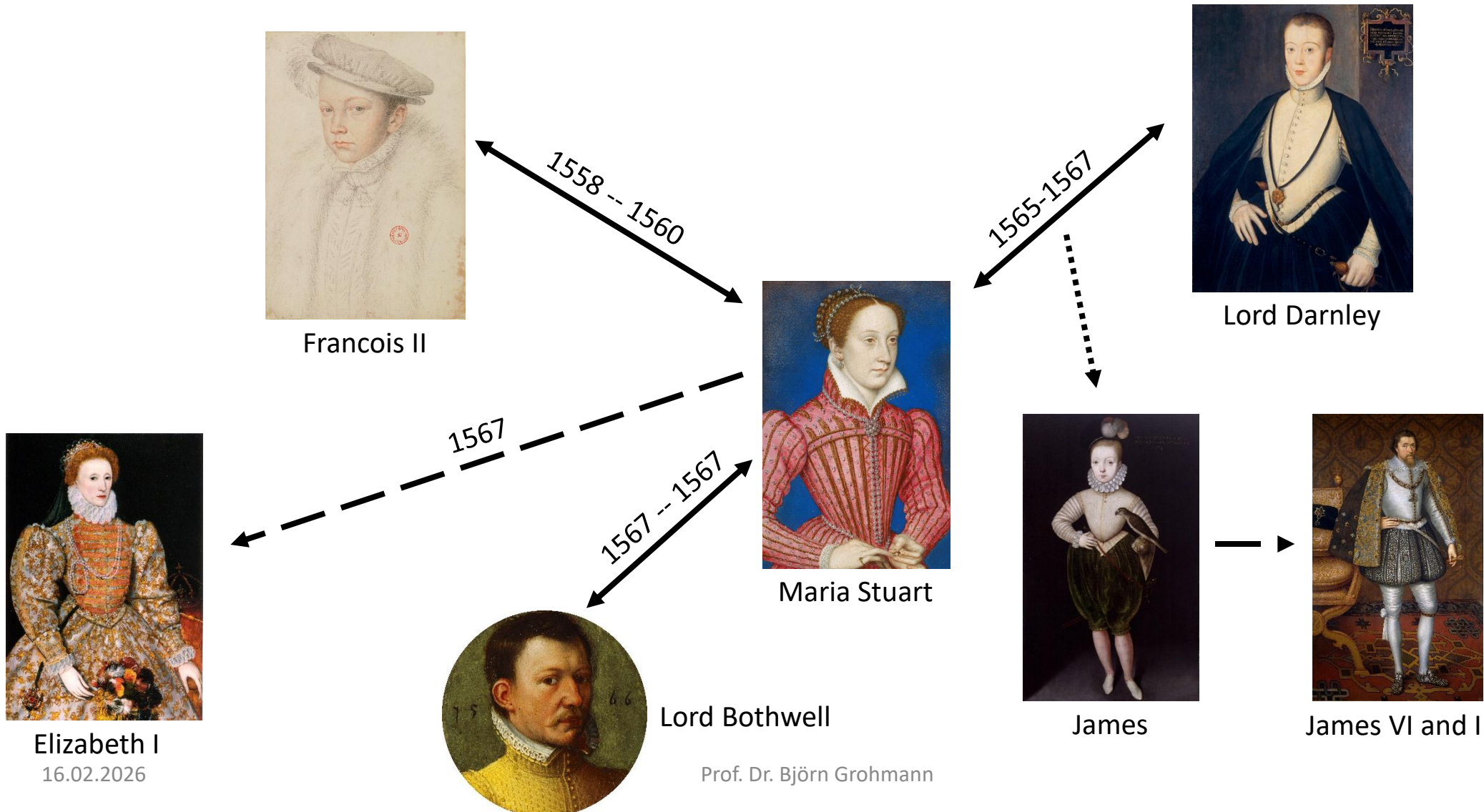
Queen of Scotland

14. Dezember 1542 -- 1567

THE QUEEN OF SCOTS

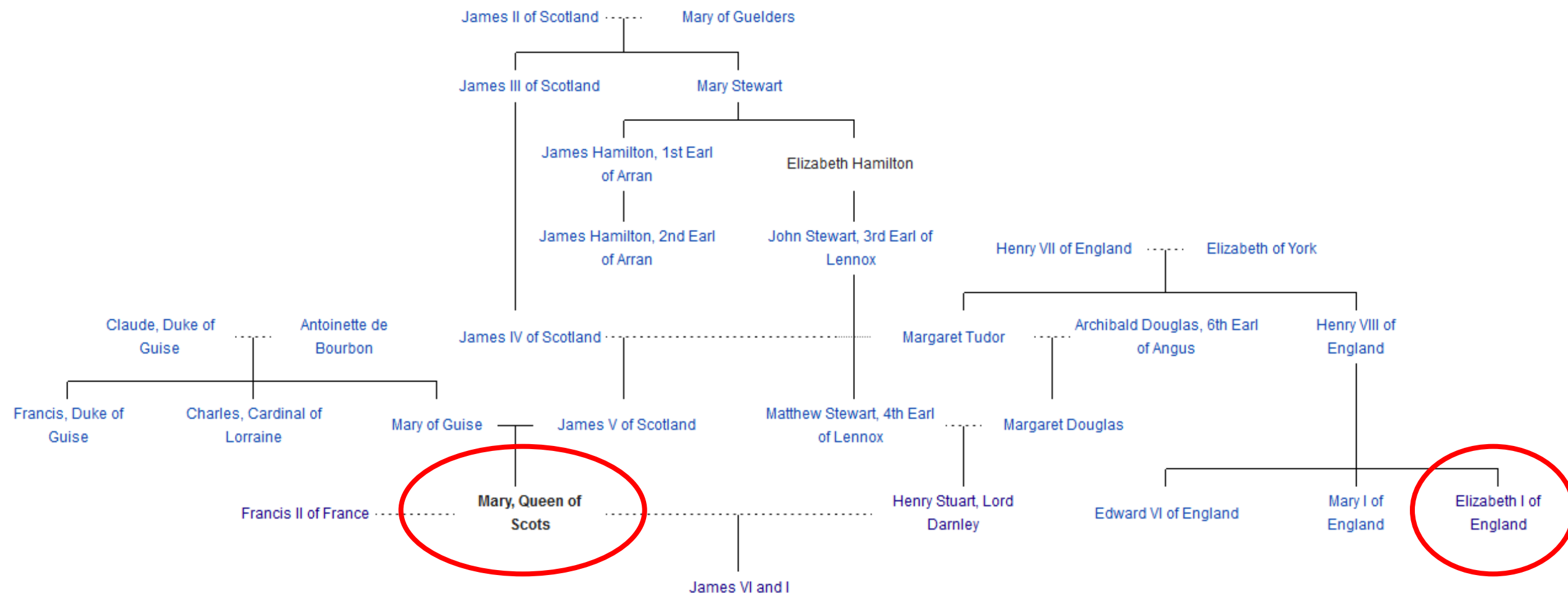


Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

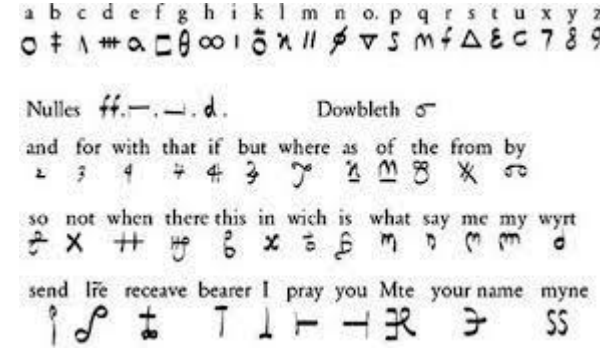
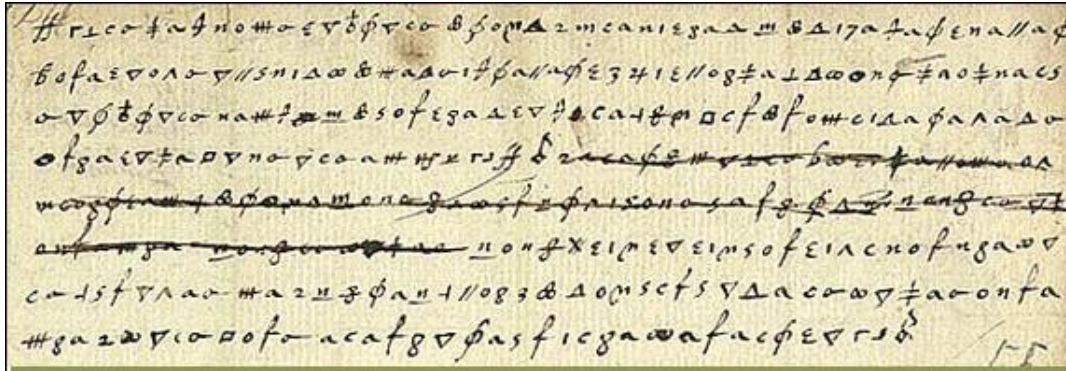




THE QUEEN OF SCOTS



THE PLOT (1586)



Anthony Babington



Maria Stuart



Gilbert Gifford



Beer barrel

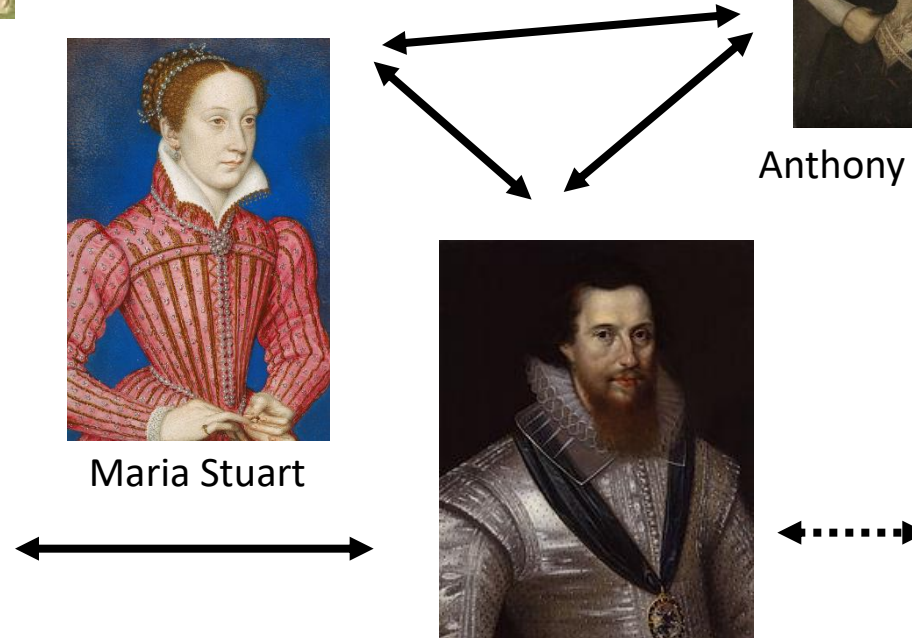
Thomas Phelippes



Elizabeth I



Sir Francis Walsingham



THE EXECUTION (1587)



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Am 8. Februar 1587 wurde **Maria Stuart** vor den Augen von 300 Schaulustigen enthauptet.

WAS LIEF HIER SCHIEF?



Für eine sichere Kommunikation fehlte z.B.

Vertraulichkeit (Confidentiality)

Integrität (Integrity)

Authentizität (Authenticity)

...und noch einige andere...

WAS LIEF HIER SCHIEF?



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

a b c d e f g h i k l m n o. p q r s t u x y z
o ‡ 1 # a □ θ ∞ i ð κ || ø ∇ s m f Δ ε c 7 8 9

Nulles ff. —, —, d. Dowbleth σ

and for with that if but where as of the from by
z 3 4 7 4 3 j n m 8 x o

so not when there this in wich is what say me my wyr
f x ++ h b x e f m n m m d

send lre receave bearer I pray you Mte your name myne
i s t T L H — R 3 ss

THE FREQUENCY OF LETTERS OF THE ENGLISH ALPHABETH



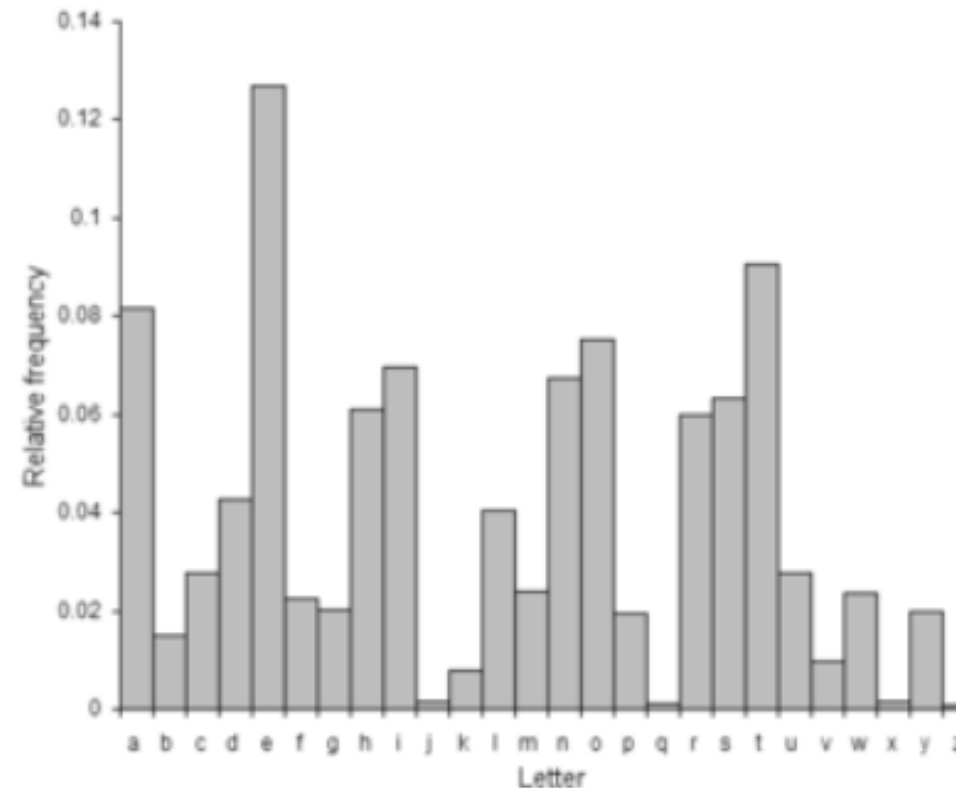
Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Samuel Morse (1791-1872)	12,000	E	2,500	F
	9,000	T	2,000	W, Y
	8,000	A, I, N, O, S	1,700	G, P
	6,400	H	1,600	B
	6,200	R	1,200	V
	4,400	D	800	K
	4,000	L	500	Q
	3,400	U	400	J, X
	3,000	C, M	200	Z

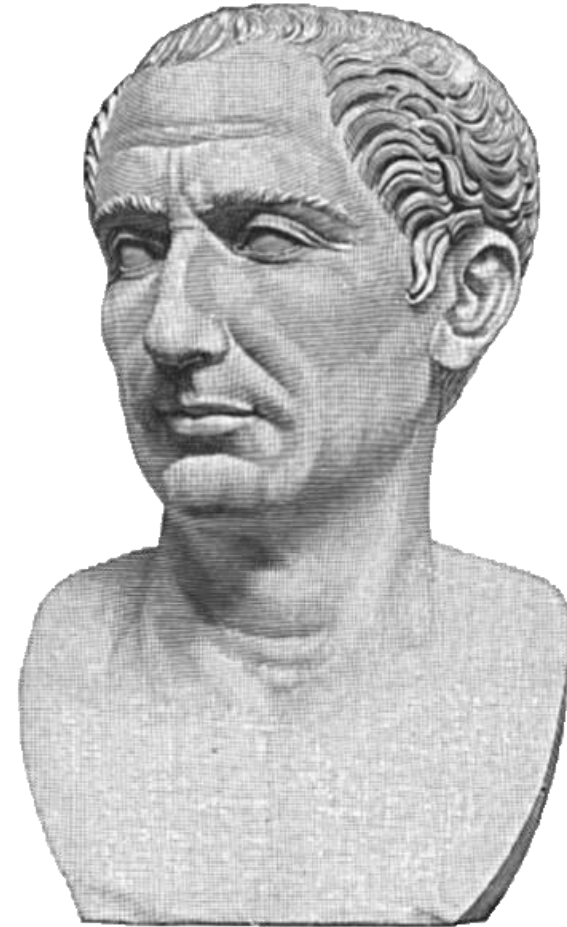
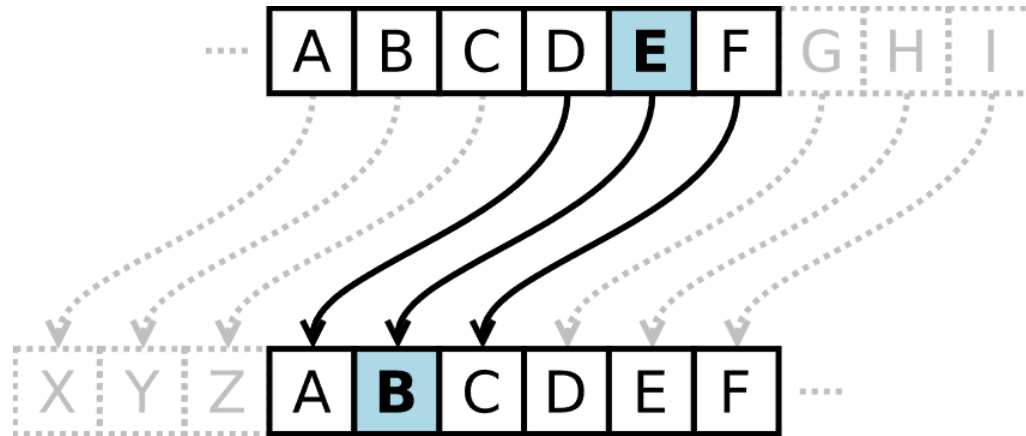
THE FREQUENCY OF LETTERS OF THE ENGLISH ALPHABETH



E	11.1607%	56.88	M	3.0129%	15.36
A	8.4966%	43.31	H	3.0034%	15.31
R	7.5809%	38.64	G	2.4705%	12.59
I	7.5448%	38.45	B	2.0720%	10.56
O	7.1635%	36.51	F	1.8121%	9.24
T	6.9509%	35.43	Y	1.7779%	9.06
N	6.6544%	33.92	W	1.2899%	6.57
S	5.7351%	29.23	K	1.1016%	5.61
L	5.4893%	27.98	V	1.0074%	5.13
C	4.5388%	23.13	X	0.2902%	1.48
U	3.6308%	18.51	Z	0.2722%	1.39
D	3.3844%	17.25	J	0.1965%	1.00
P	3.1671%	16.14	Q	0.1962%	(1)



CEASAR CIPHER

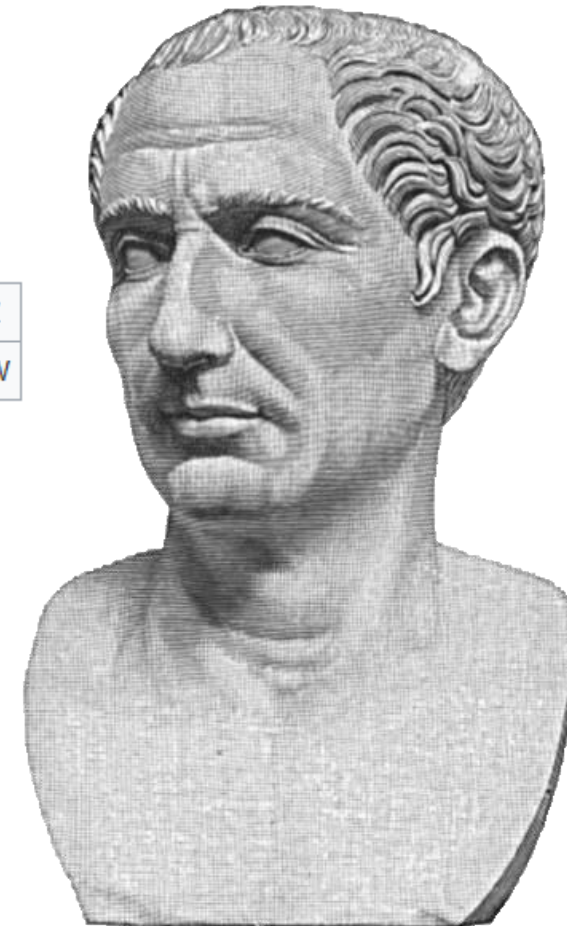


CEASAR CIPHER



Plain	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
Cipher	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

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD



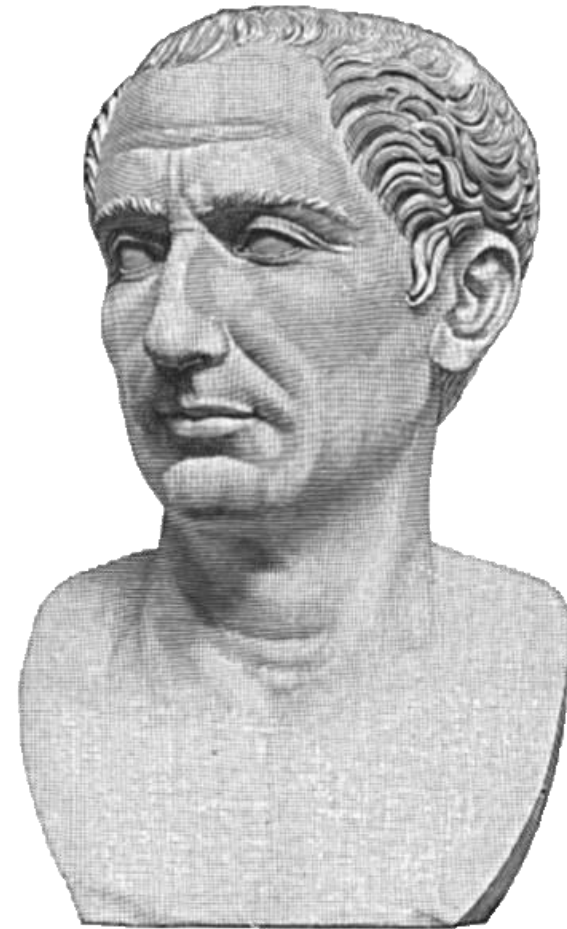
CEASAR CIPHER



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

$$E_n(x) = x + n \bmod 26$$

$$D_n(x) = x - n \bmod 26$$



VIGENERE CIPHER



	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



VIGENERE CIPHER



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Plaintext: `attackatdawn`

Key: `LEMONLEMONLE`

Ciphertext: `LXFOPVEFRNHR`



VIGENERE CIPHER



$$C_i = E_K(M_i) = M_i + K_i \bmod 26$$

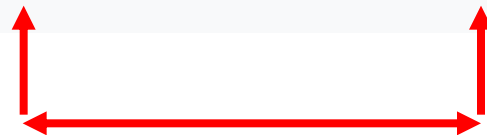
$$M_i = D_K(C_i) = C_i - K_i \bmod 26$$



VIGENERE CIPHER



Key: ABCDABCDABCDABCDABCDABCDABCD
Plaintext: cryptoisshortforcryptography
Ciphertext: CSASTPKVSIQUTGQUCSASTPIUAQJB



Distance is 16,
so the key-length
is probably
1, 2, 4, 8 or 16



OTHER ATTEMPTS (HOMOPHONIC CIPHERS)

A.	B.	C.	D.	E.	F.	G.	H.	I.	K.	L.	M.	N.	O.	P.	Q.	R.	S.	T.	V.	W.	X.	Y.	Z.
4.	14.	24.	34.	44.	54.	64.	74.	84.	94.	104.	114.	124.	134.	144.	154.	164.	174.	184.	194.	204.	214.	224.	234.
235.	225.	215.	205.	195.	185.	175.	165.	155.	145.	135.	125.	115.	105.	95.	85.	75.	65.	55.	45.	35.	25.	15.	5.
7.	17.	27.	37.	47.	57.	67.	77.	87.	97.	107.	117.	127.	137.	147.	157.	167.	177.	187.	197.	207.	217.	227.	237.

Da.	De.	Di.	Do.	Da.	Ta.	To.	Ti.	To.	Ta.	Ge.	Gi.	To.	Ha.	He.	Hi.	Ho.	Ha.	Ka.	Ke.	Ki.	Ko.	Ku.	La.	Li.	Lo.	Lu.
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.	27.
28.	29.	30.	31.	32.	33.	34.	35.	36.	37.	38.	39.	40.	41.	42.	43.	44.	45.	46.	47.	48.	49.	50.	51.	52.	53.	54.
55.	56.	57.	58.	59.	60.	61.	62.	63.	64.	65.	66.	67.	68.	69.	70.	71.	72.	73.	74.	75.	76.	77.	78.	79.	80.	

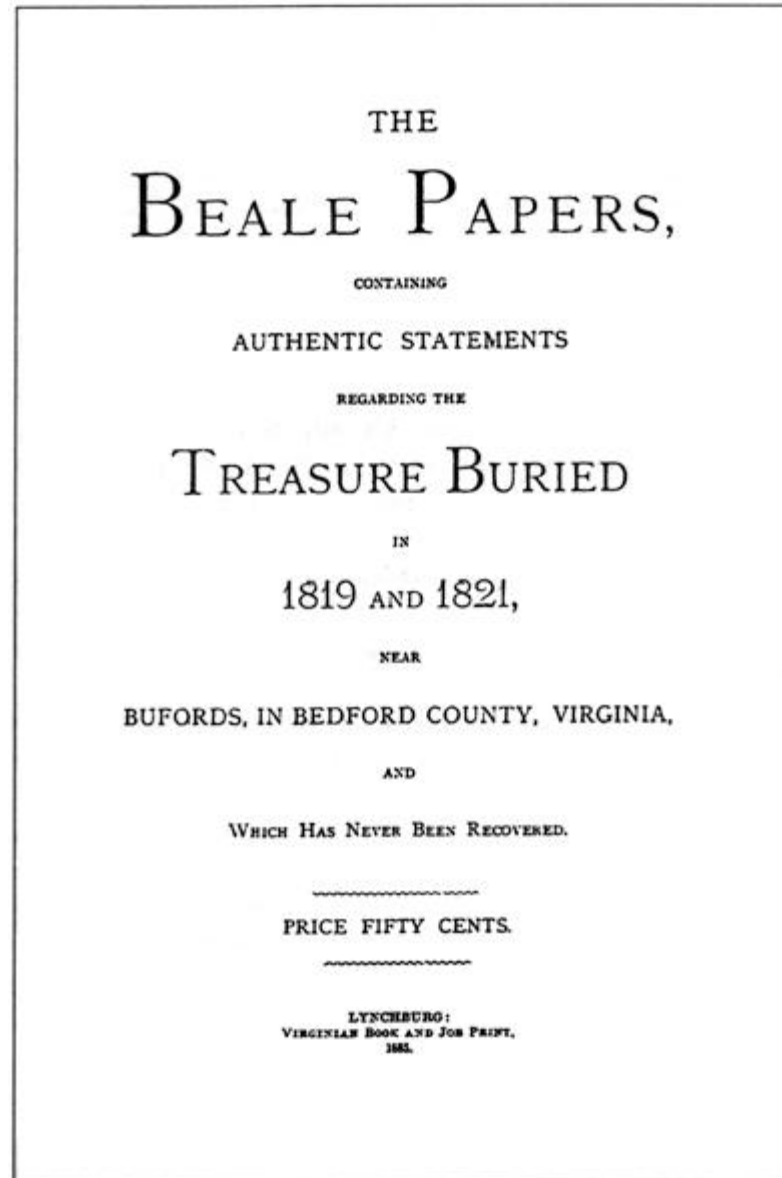
Ma.	Me.	Mo.	Ma.	Na.	Ne.	Ni.	Na.	Pa.	Pe.	Pi.	Pa.	Ra.	Re.	Ri.	Ra.	Sa.	Se.	Si.	So.	Ta.	Te.	Ti.	To.	Wa.	We.	Wi.	Wo.	Wa.
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.	
29.	30.	31.	32.	33.	34.	35.	36.	37.	38.	39.	40.	41.	42.	43.	44.	45.	46.	47.	48.	49.	50.	51.	52.	53.	54.	55.		
56.	57.	58.	59.	60.	61.	62.	63.	64.	65.	66.	67.	68.	69.	70.	71.	72.	73.	74.	75.	76.	77.	78.	79.	80.	81.	82.		

F.	L.	O.	R.	S.	V.	Z.
1.	2.	3.	4.	5.	6.	7.
8.	9.	10.	11.	12.	13.	14.
15.	16.	17.	18.	19.	20.	21.

B.	D.	H.	J.	N.	Q.	T.	W.
1.	2.	3.	4.	5.	6.	7.	8.
9.	10.	11.	12.	13.	14.	15.	16.
17.	18.	19.	20.	21.	22.	23.	24.

218

WANT TO
BECOME
RICH?



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

WANT TO BECOME RICH?



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975, 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485, 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283, 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62, 116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461, 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86, 36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62, 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895, 10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62, 31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31, 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216, 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56, 216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617, 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132, 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936, 447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216, 814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84, 221, 736, 820, 214, 11, 60, 760.

Ciphertext 1

Hier steht „wo“ der Schatz ist

317, 8, 92, 73, 112, 89, 67, 318, 28, 96, 107, 41, 631, 78, 146, 397, 118, 98, 114, 246, 348, 116, 74, 88, 12, 65, 32, 14, 81, 19, 76, 121, 216, 85, 33, 66, 15, 108, 68, 77, 43, 24, 122, 96, 117, 36, 211, 301, 15, 44, 11, 46, 89, 18, 136, 68, 317, 28, 90, 82, 304, 71, 43, 221, 198, 176, 310, 319, 81, 99, 264, 380, 56, 37, 319, 2, 44, 53, 28, 44, 75, 98, 102, 37, 85, 107, 117, 64, 88, 136, 48, 154, 99, 175, 89, 315, 326, 78, 96, 214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84, 65, 26, 41, 246, 84, 270, 98, 116, 32, 59, 74, 66, 69, 240, 15, 8, 121, 20, 77, 89, 31, 11, 106, 81, 191, 224, 328, 18, 75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84, 35, 54, 109, 128, 49, 77, 88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311, 96, 54, 32, 120, 18, 132, 102, 219, 211, 84, 150, 219, 275, 312, 64, 10, 106, 87, 75, 47, 21, 29, 37, 81, 44, 18, 126, 115, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11, 28, 97, 318, 238, 106, 24, 93, 3, 19, 17, 26, 60, 73, 88, 14, 126, 138, 234, 286, 297, 321, 365, 264, 19, 22, 84, 56, 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28, 46, 42, 107, 196, 227, 344, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6, 328, 65, 48, 52, 59, 41, 122, 33, 117, 11, 18, 25, 71, 36, 45, 83, 76, 89, 92, 31, 65, 70, 83, 96, 27, 33, 44, 50, 61, 24, 112, 136, 149, 176, 180, 194, 143, 171, 205, 296, 87, 12, 44, 51, 89, 98, 34, 41, 208, 173, 66, 9, 35, 16, 95, 8, 113, 175, 90, 56, 203, 19, 177, 183, 206, 157, 200, 218, 260, 291, 305, 618, 951, 320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84, 96, 207, 244, 66, 82, 119, 71, 11, 86, 77, 213, 54, 82, 316, 245, 303, 86, 97, 106, 212, 18, 37, 15, 81, 89, 16, 7, 81, 39, 96, 14, 43, 216, 118, 29, 55, 109, 136, 172, 213, 64, 8, 227, 304, 611, 221, 364, 819, 375, 128, 296, 1, 18, 53, 76, 10, 15, 23, 19, 71, 84, 120, 134, 66, 73, 89, 96, 230, 48, 77, 26, 101, 127, 936, 218, 439, 178, 171, 61, 226, 313, 215, 102, 18, 167, 262, 114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119, 34, 127, 139, 34, 128, 129, 74, 63, 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124, 265, 89, 96, 126, 274, 896, 917, 434, 461, 235, 890, 312, 413, 328, 381, 96, 105, 217, 66, 118, 22, 77, 64, 42, 12, 7, 55, 24, 83, 67, 97, 109, 121, 135, 181, 203, 219, 228, 256, 21, 34, 77, 319, 374, 382, 675, 684, 717, 864, 203, 4, 18, 92, 16, 63, 82, 22, 46, 55, 69, 74, 112, 134, 186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218, 343, 417, 845, 951, 124, 209, 49, 617, 856, 924, 936, 72, 19, 28, 11, 35, 42, 40, 66, 85, 94, 112, 65, 82, 115, 119, 236, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72, 32, 47, 63, 96, 124, 217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22, 18, 46, 137, 181, 101, 39, 86, 103, 116, 138, 164, 212, 218, 296, 815, 380, 412, 460, 495, 675, 820, 952.

Ciphertext 3

Hier steht „wer“ ihn kriegen soll

WANT TO BECOME RICH?

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56, 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122, 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41, 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196, 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6, 191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46, 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113, 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107, 603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8, 14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53, 79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 505, 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115, 48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121, 12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41, 85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49, 47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2, 270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31, 10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250, 557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106, 160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353, 320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11, 110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27, 8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51, 50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140, 112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150, 112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811, 30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205, 185, 112, 125, 540, 65, 106, 807, 138, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50, 154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205, 38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37, 38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84, 125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30, 150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140, 485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811, 125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302, 246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51, 63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

Hier steht
„was“ der
Schatz ist

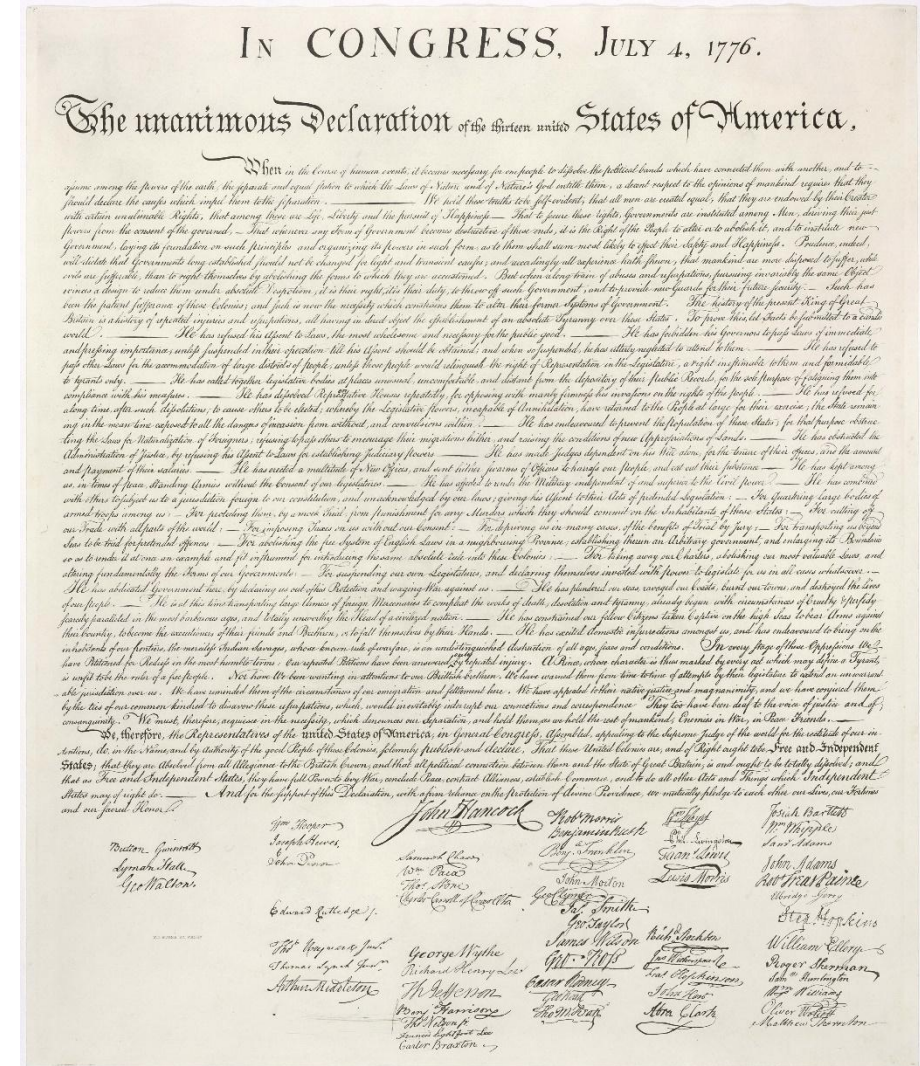
Ciphertext 2

16.02.2026

Prof. Dr. Björn Grohmann



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



21

WANT TO BECOME RICH?



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

I have deposited in the county of Bedford, about four miles from Buford's, in an excavation or vault, six feet below the surface of the ground, the following articles, belonging jointly to the parties whose names are given in number three, herewith:

The first deposit consisted of ten hundred and fourteen pounds of gold, and thirty-eight hundred and twelve pounds of silver, deposited Nov. eighteen nineteen. The second was made Dec. eighteen twenty-one, and consisted of nineteen hundred and seven pounds of gold, and twelve hundred and eighty-eight of silver, also jewels, obtained in St. Louis in exchange to save transportation, and valued at thirteen thousand dollars.

The above is securely packed in iron pots, with iron covers. The vault is roughly lined with stone, and the vessels rest on solid stone, and are covered with others. Paper number one describes the exact locality of the vault, so that no difficulty will be had in finding it.

WIE MISST MAN (EIGENTLICH) SICHERHEIT? (1. ANSATZ)



Claude Shannon 1916-2001

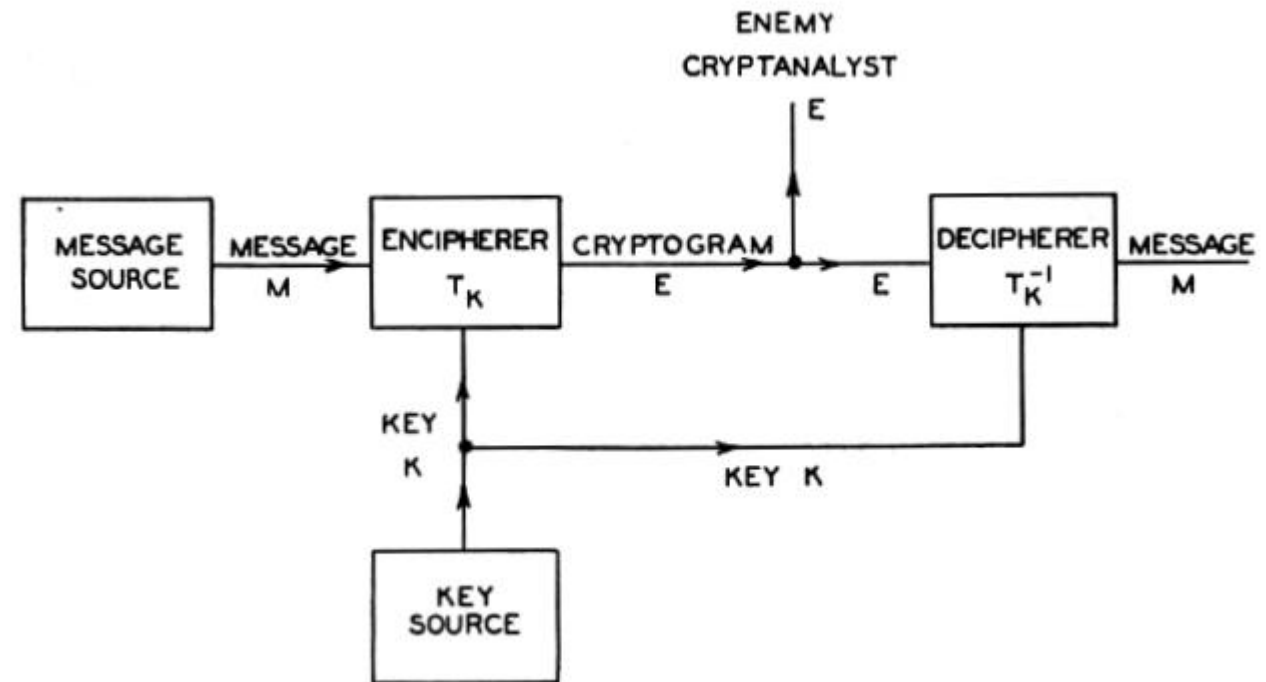


Fig. 1—Schematic of a general secrecy system.

WIE MISST MAN (EIGENTLICH) SICHERHEIT? (1. ANSATZ)



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Claude Shannon 1916-2001

Das ist genau dann der Fall,
falls M und E stochastisch
unabhängig sind

A system has perfect secrecy, if and only if

$$H(M|E) = H(M),$$

where $H(\cdot)$ (resp. $H(\cdot, \cdot)$) denotes the (conditional) Entropy-function.

WIE MISST MAN (EIGENTLICH) SICHERHEIT? (1. ANSATZ)



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



Claude Shannon 1916-2001

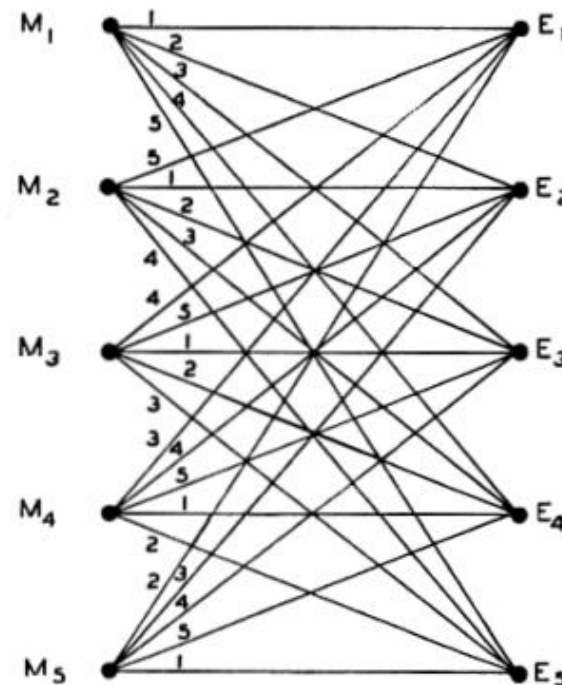
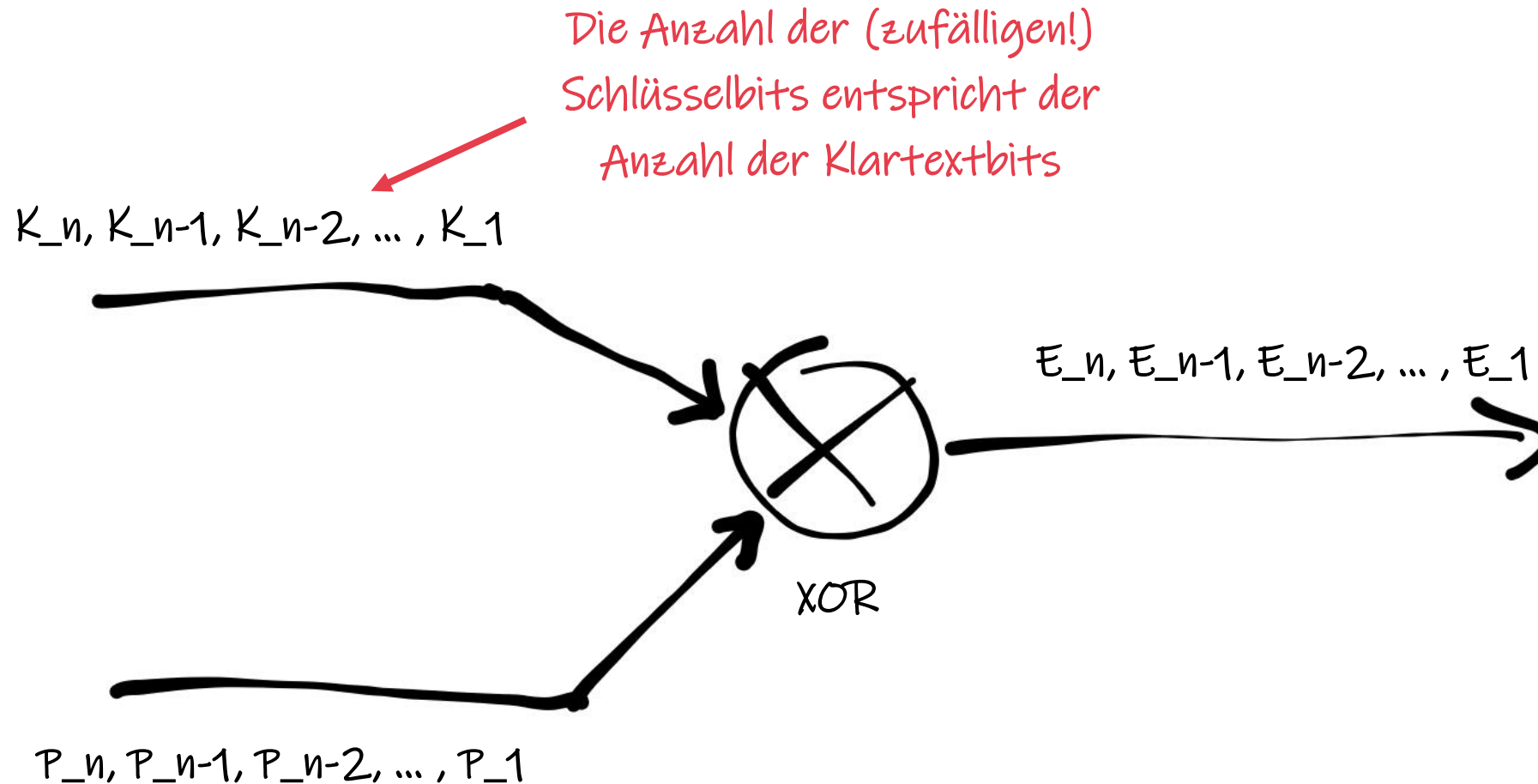


Fig. 5—Perfect system.

...jeder Chiffretext ist
(unabhängig vom Klartext)
gleich wahrscheinlich

ONE TIME PAD



SYMMETRISCHE CHIFFRE

Man nennt eine Chiffre **symmetrisch**, wenn für die Verschlüsselung und die Entschlüsselung **das selbe Schlüsselmaterial** genutzt wird

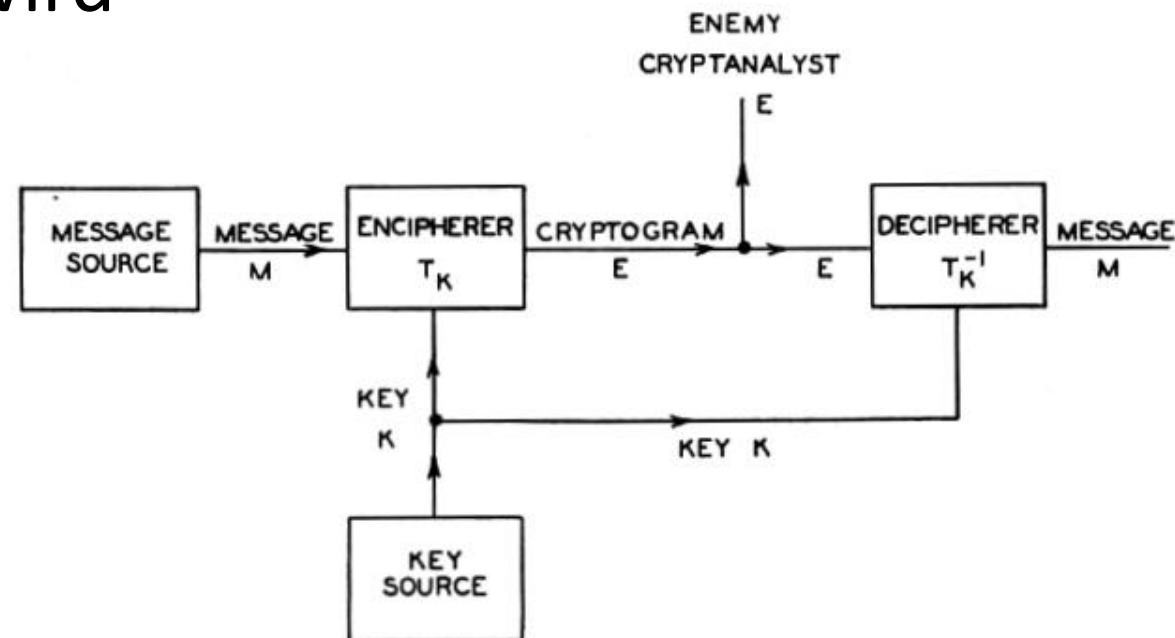
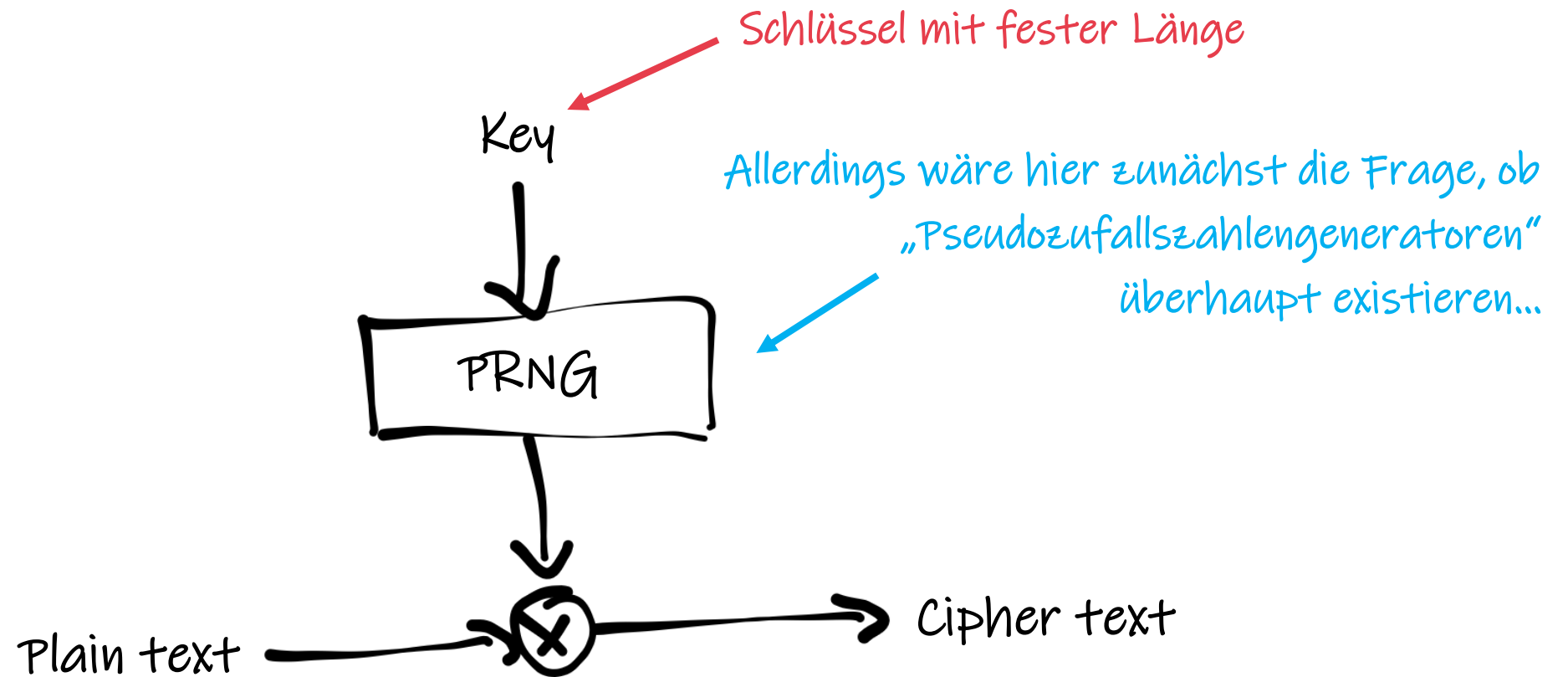


Fig. 1—Schematic of a general secrecy system.

STROM-CHIFFRE



PSEUDORANDOM GENERATORS



Definition (**PseudoRandom Generator** – PRG): *The function $G : \{0, 1\}^* \rightarrow \{0, 1\}^*$ with stretch function $l(n)$ is a pseudo-random generator if:*

- G is a **polynomial time** algorithm
- for every x , $|G(x)| = l(|x|) > |x|$
- $\{G(U_n)\}$ and $\{U_{l(n)}\}$ are computational indistinguishable, where U_m denotes the **uniform distribution** over $\{0, 1\}^m$.

PSEUDORANDOM GENERATORS



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

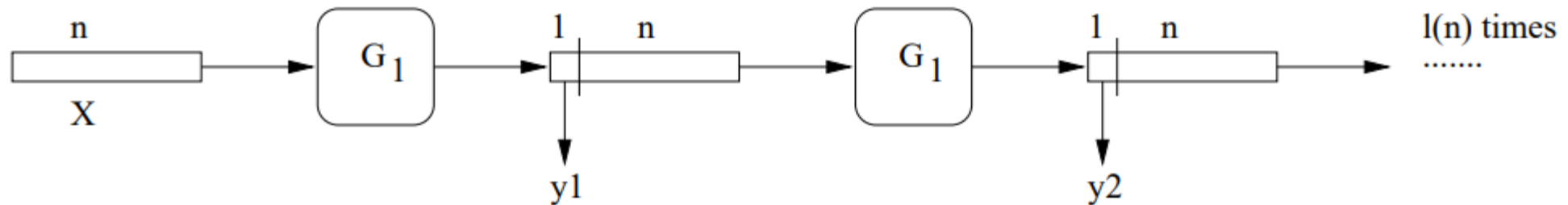
Definition 13.4 (canonic notion of computational indistinguishability): *Two probability ensembles $\{X_n\}_{n \in \mathbb{N}}$ and $\{Y_n\}_{n \in \mathbb{N}}$ are computationally indistinguishable if they are indistinguishable by any probabilistic polynomial-time algorithm. That is, for every probabilistic polynomial-time algorithm A , and every polynomial $p()$ there exists N s.t. for all $n > N$*

$$|\Pr(A(X_n) = 1) - \Pr(A(Y_n) = 1)| < \frac{1}{p(n)}$$

PSEUDORANDOM GENERATORS



Theorem 13.10 (amplification of stretch function): *Suppose we have a Pseudo-Random Generator G_1 with a stretch function $n + 1$. Then for all polynome $l(n)$ there exists a Pseudo-Random Generator with stretch function $l(n)$.*



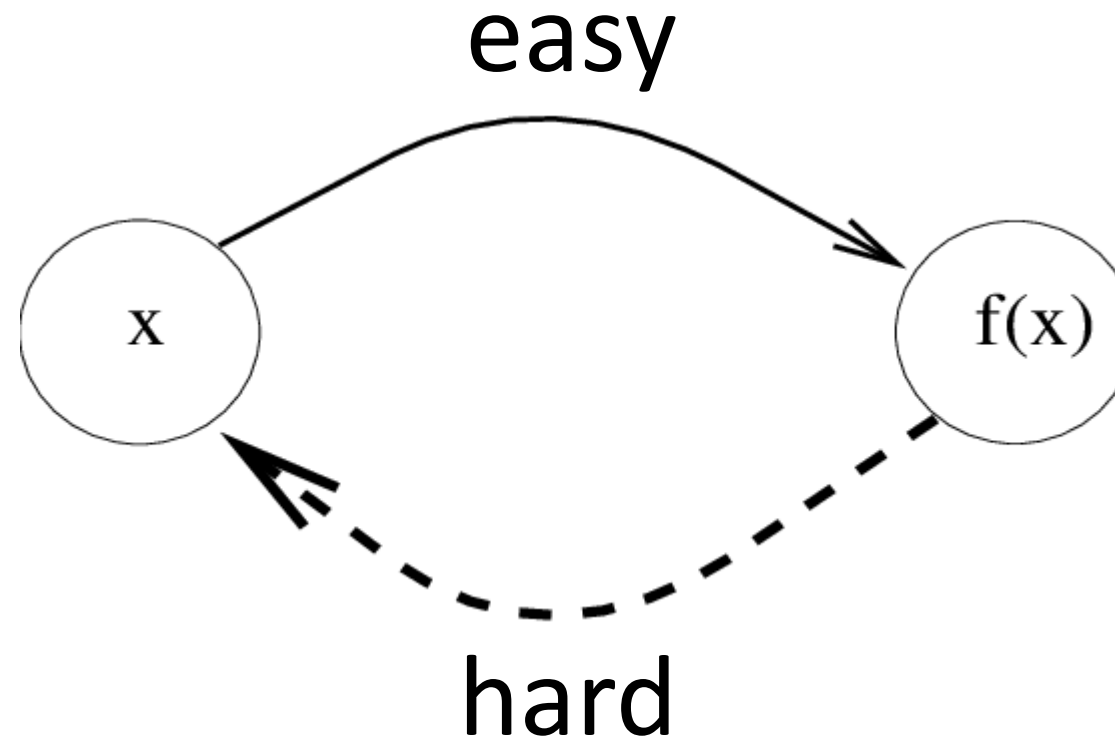
PSEUDORANDOM GENERATORS



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Theorem *Pseudo-Random Generators exist if and only if One-Way Functions exist.*

ONE-WAY FUNCTION



ONE-WAY FUNCTION



Definition 13.11 (**One-way functions** – OWF): A function $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ such that $\forall x |f(x)| = |x|$ is one-way if :

- there is exists **polynomial time** algorithm A , such that $\forall x A(x) = f(x)$
- for all probabilistic polynomial time A' and for all polynome $p()$ and for all sufficiently large n 's :

$$\Pr \left[A'(f(U_n)) = f^{-1} \circ f(U_n) \right] < \frac{1}{p(n)}$$

Diese
Bedingung
kann auch
abgeschwächt
werden...

OWF vs PRNG



PRG \rightarrow OWF: Consider pseudo-random generator $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$. Let us define function $f : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ as follows:

$$f(xy) = G(x) \quad (|x| = |y| = n).$$

Wenn das ein PRNG ist...

...dann ist das eine OWF

OWF vs PRNG



Definition 13.13 (Hardcore):

Let f be one-way function, $b : \{0, 1\}^* \longrightarrow \{0, 1\}$ is a hardcore of f if:

- \exists polynomial time algorithm A , such that $\forall t A(t) = b(t)$
- \forall probabilistic polynomial time algorithm $A' \forall$ polynom $p(.) \forall$ sufficiently large n 's

$$\Pr [A'(f(U_n)) = b(U_n)] < \frac{1}{2} + \frac{1}{p(n)}$$

In other words this function must be easy to compute and hard to predict out of $f(x)$.

OWF vs PRNG



OWF \rightarrow PRG:

(hier ist zudem die Annahme, dass f bijektiv ist)

Theorem 2.3 Suppose that f is a one-way function. Let $f'(x, r) = (f(x), r)$, and $b(x, r)$ be the inner-product mod 2 of x and r . Then b is a hardcore predicate of f' .

$$G(s) = f'(s) \circ b(s)$$

Wenn das eine OWF ist...
...und das ein HCP...
...dann ist das ein PRNG.

ANWENDUNGEN



Lamport's One-Time-Signature

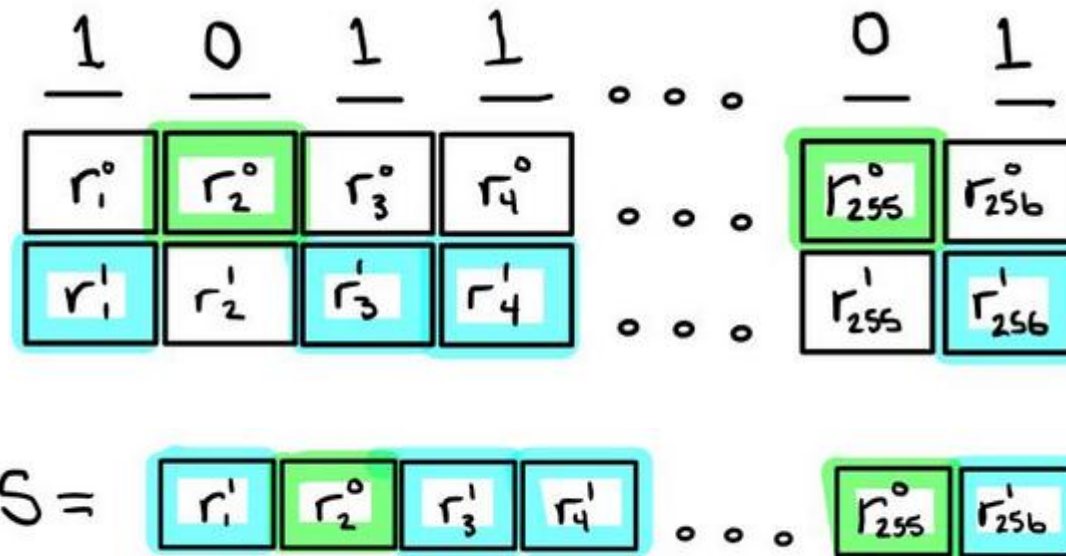
...das untere ist das
Bild des oberen
mittels einer OWF.

$$\begin{aligned} SK = & \begin{array}{cccc} r_1^0 & r_2^0 & r_3^0 & r_4^0 \\ r_1^1 & r_2^1 & r_3^1 & r_4^1 \end{array} \quad \circ \quad \circ \quad \circ \quad \begin{array}{cc} r_{255}^0 & r_{256}^0 \\ r_{255}^1 & r_{256}^1 \end{array} \\ PK = & \begin{array}{cccc} y_1^0 & y_2^0 & y_3^0 & y_4^0 \\ y_1^1 & y_2^1 & y_3^1 & y_4^1 \end{array} \quad \circ \quad \circ \quad \circ \quad \begin{array}{cc} y_{255}^0 & y_{256}^0 \\ y_{255}^1 & y_{256}^1 \end{array} \end{aligned}$$

ANWENDUNGEN



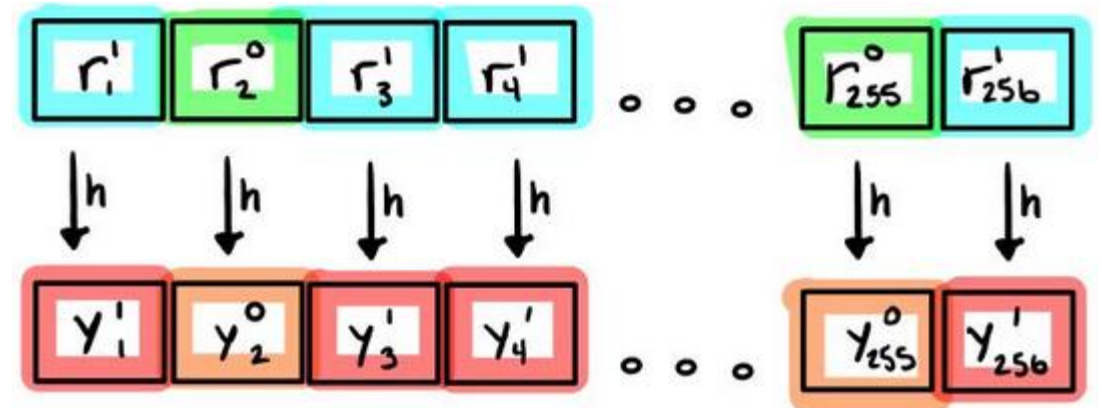
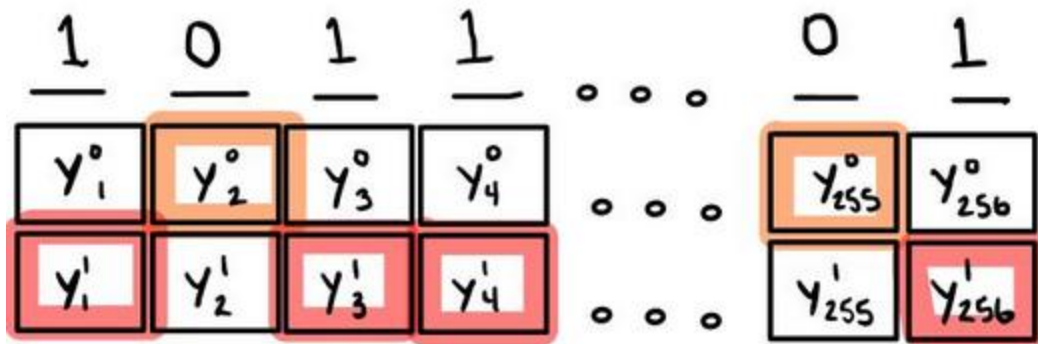
Lamport's One-Time-Signature



ANWENDUNGEN



Lamport's One-Time-Signature



ANWENDUNGEN



A *bit commitment* protocol consists of two stages:

- The *commit stage*: Alice has a bit b to which she wishes to commit to Bob. She and Bob exchange messages. At the end of the stage Bob has some information that represents b .
- The *revealing stage*: at the end of which Bob knows b .

1. After the commit stage Bob cannot guess b with probability greater than $\frac{1}{2} + \frac{1}{p(n)}$.
2. Alice can reveal only one possible value. If she tries to reveal a different value she is caught with probability at least $1 - \frac{1}{p(n)}$.

ANWENDUNGEN



Erste Idee...

- Commit stage - Alice selects seed $s \in \{0, 1\}^n$ and sends $G_m(s)$ and $B_{m+1}(s) \oplus b$.
(b is the bit Alice is committed to.)
- Reveal stage - Alice sends s , Bob verifies that $G_m(s)$ is what Alice sent him before and computes $b = B_{m+1}(s) \oplus (B_{m+1}(s) \oplus b)$

die ersten m Bits von $G(s)$,
wobei G ein PRNG

das $m+1^{\text{ste}}$ Bit von $G(s)$

Alice might be able to cheat: if she finds two seeds s_1 and s_2 such that $G_m(s_1) = G_m(s_2)$, but $B_{m+1}(s_1) \neq B_{m+1}(s_2)$, then she can reveal any bit she wishes (by sending s_1 or s_2). There is nothing in the definition of pseudo-random generators that forbids



Bessere Idee...(?)

- Commit stage -

1. Bob selects a random vector $\vec{R} = (r_1, r_2, \dots, r_{3n})$ where $r_i \in \{0, 1\}$ for $1 \leq i \leq 3n$ and sends it to Alice.
2. Alice selects a seed $s \in \{0, 1\}^n$ and sends to Bob the vector $\vec{D} = (d_1, d_2, \dots, d_{3n})$ where

$$d_i = \begin{cases} B_i(s) & \text{if } r_i = 0 \\ B_i(s) \oplus b & \text{if } r_i = 1 \end{cases}$$

- Reveal stage - Alice sends s and Bob verifies that for all $1 \leq i \leq 3n$, if $r_i = 0$ then $d_i = B_i(s)$, and if $r_i = 1$ then $c_i = B_i(s) \oplus b$.



How can Alice cheat? Her only chance to cheat is if there exist two seeds s_1 and s_2 such that $G_{3n}(s_1)$ and $G_{3n}(s_2)$ agree in all positions i where $r_i = 0$, and totally disagree in all positions i where $r_i = 1$. We say that such a pair fools \vec{R} .

Claim 3.1 *The **Probability** that there exists a pair of seeds s_1 and s_2 that fools \vec{R} is at most 2^{-n} , where the probability is taken over the choices of \vec{R} .*

Proof: If a pair s_1, s_2 fools \vec{R} , then we know that $r_i = B_i(s_1) \oplus B_i(s_2)$. Therefore, a pair s_1 and s_2 fools exactly one \vec{R} . There are 2^{2n} pairs of seeds and 2^{3n} vectors \vec{R} . Hence the probability that there exists a pair that can fool the \vec{R} that Bob chose is at most $\frac{2^{2n}}{2^{3n}} = 2^{-n}$. \square

ZURÜCK ZU DEN STROMCHIFFREN: CHACHA20



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

The inputs to `ChaCha20` are:

- o A 256-bit key
- o A 32-bit initial counter. This can be set to any number, but will usually be zero or one. It makes sense to use one if we use the zero block for something else, such as generating a one-time authenticator key as part of an AEAD algorithm.
- o A 96-bit nonce. In some protocols, this is known as the Initialization Vector.
- o An arbitrary-length plaintext

The output is an encrypted message, or "ciphertext", of the same length.

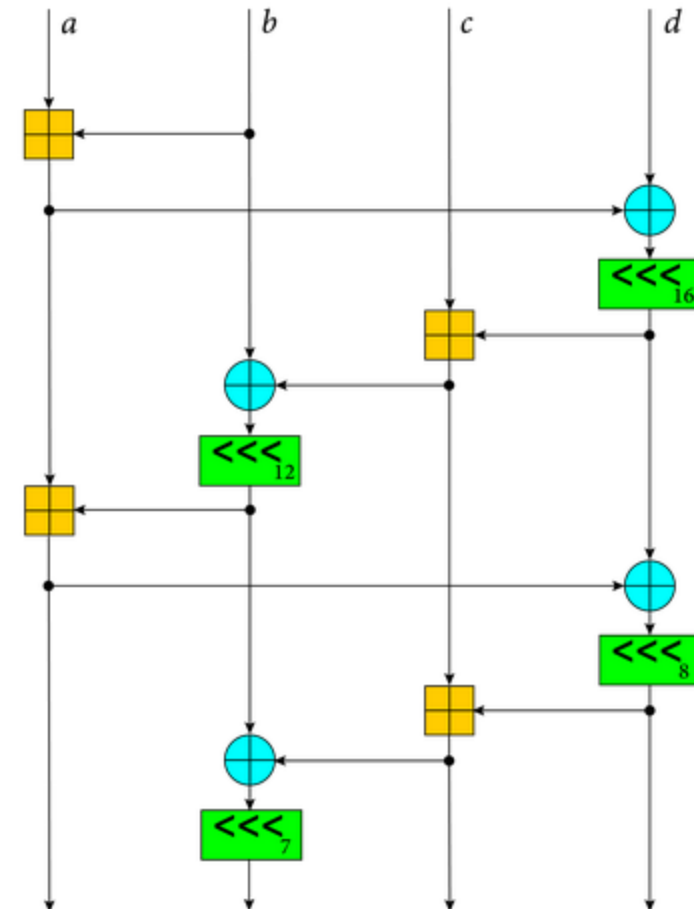
ZURÜCK ZU DEN STROMCHIFFREN: CHACHA20



2.1. The ChaCha Quarter Round

The basic operation of the ChaCha algorithm is the quarter round. It operates on four 32-bit unsigned integers, denoted a , b , c , and d . The operation is as follows (in C-like notation):

1. $a \oplus= b$; $d \oplus= a$; $d \lll= 16$;
2. $c \oplus= d$; $b \oplus= c$; $b \lll= 12$;
3. $a \oplus= b$; $d \oplus= a$; $d \lll= 8$;
4. $c \oplus= d$; $b \oplus= c$; $b \lll= 7$;



ZURÜCK ZU DEN STROMCHIFFREN: CHACHA20



2.1. The ChaCha Quarter Round

The basic operation of the ChaCha algorithm is the quarter round. It operates on four 32-bit unsigned integers, denoted a, b, c, and d. The operation is as follows (in C-like notation):

1. $a += b$; $d ^= a$; $d \lll 16$;
2. $c += d$; $b ^= c$; $b \lll 12$;
3. $a += b$; $d ^= a$; $d \lll 8$;
4. $c += d$; $b ^= c$; $b \lll 7$;

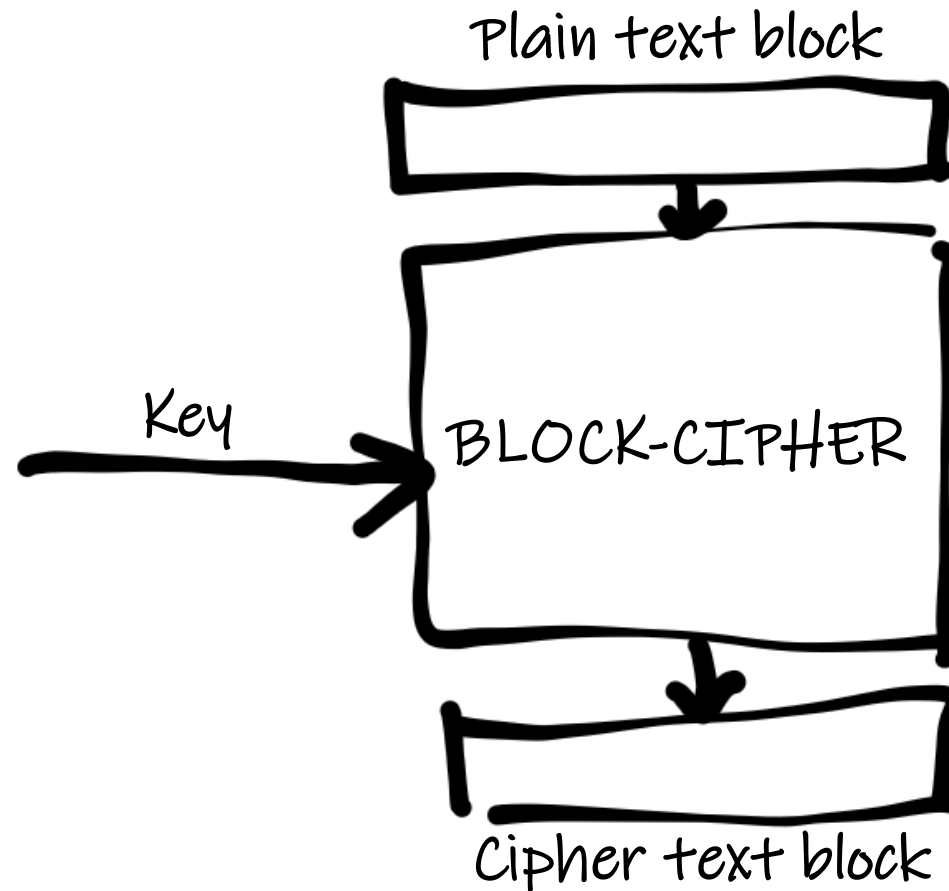
```
inner_block (state):  
  Qround(state, 0, 4, 8,12)  
  Qround(state, 1, 5, 9,13)  
  Qround(state, 2, 6,10,14)  
  Qround(state, 3, 7,11,15)  
  Qround(state, 0, 5,10,15)  
  Qround(state, 1, 6,11,12)  
  Qround(state, 2, 7, 8,13)  
  Qround(state, 3, 4, 9,14)  
end
```

```
chacha20_block(key, counter, nonce):  
  state = constants | key | counter | nonce  
  working_state = state  
  for i=1 upto 10  
    inner_block(working_state)  
  end  
  state += working_state  
  return serialize(state)  
end
```

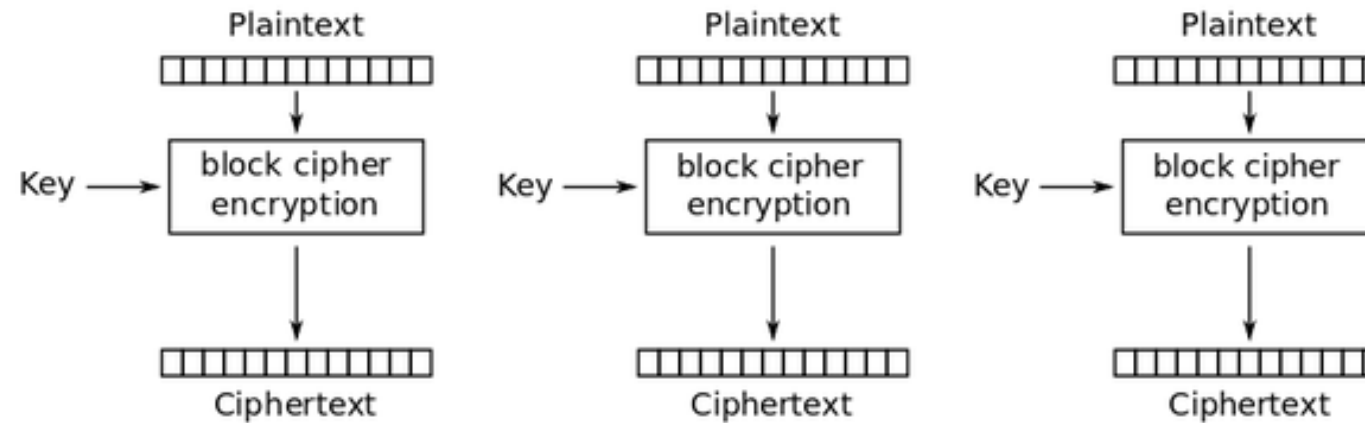
2.4.1. The ChaCha20 Encryption Algorithm in Pseudocode

```
chacha20_encrypt(key, counter, nonce, plaintext):  
  for j = 0 upto floor(len(plaintext)/64)-1  
    key_stream = chacha20_block(key, counter+j, nonce)  
    block = plaintext[(j*64)..(j*64+63)]  
    encrypted_message += block ^ key_stream  
  end  
  if ((len(plaintext) % 64) != 0)  
    j = floor(len(plaintext)/64)  
    key_stream = chacha20_block(key, counter+j, nonce)  
    block = plaintext[(j*64)..len(plaintext)-1]  
    encrypted_message += (block^key_stream)[0..len(plaintext)%64]  
  end  
  return encrypted_message  
end
```

BLOCK-CHIFFRE

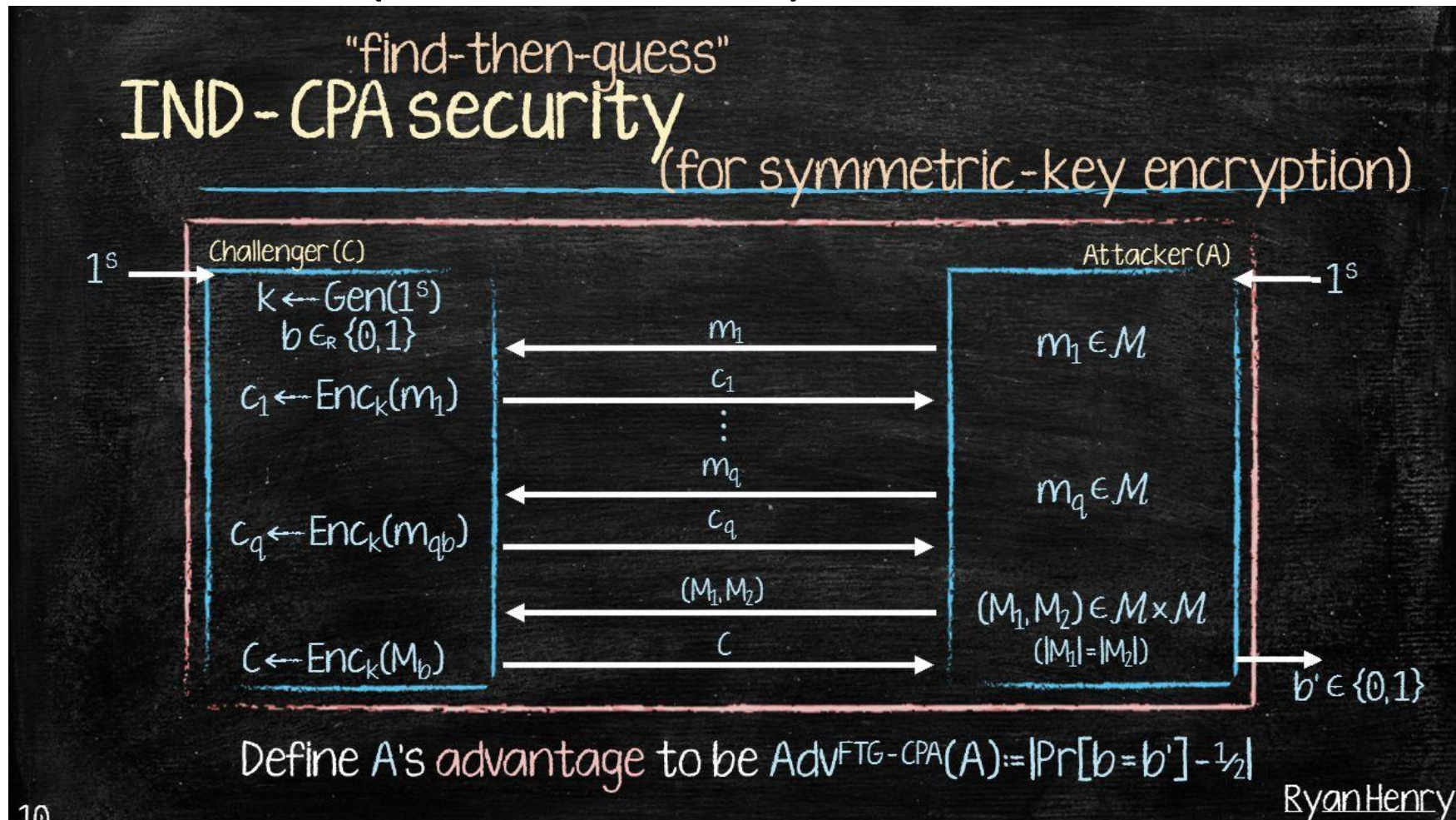


ELECTRONIC CODE BOOK



Electronic Codebook (ECB) mode encryption

WIE MISST MAN (EIGENTLICH) SICHERHEIT? (2. ANSATZ)





Ciphertext-only attack

Deduce the decryption key or plaintext by only observing the ciphertext

Known plaintext attack

Reveal further secret information by making use of samples of both plaintext and ciphertext

Chosen plaintext attack

Gain further secret information by choosing arbitrary plaintexts to be encrypted and obtaining the corresponding ciphertexts

Adaptive chosen plaintext attack

Choose subsequent plaintexts based on the information received from previous requests

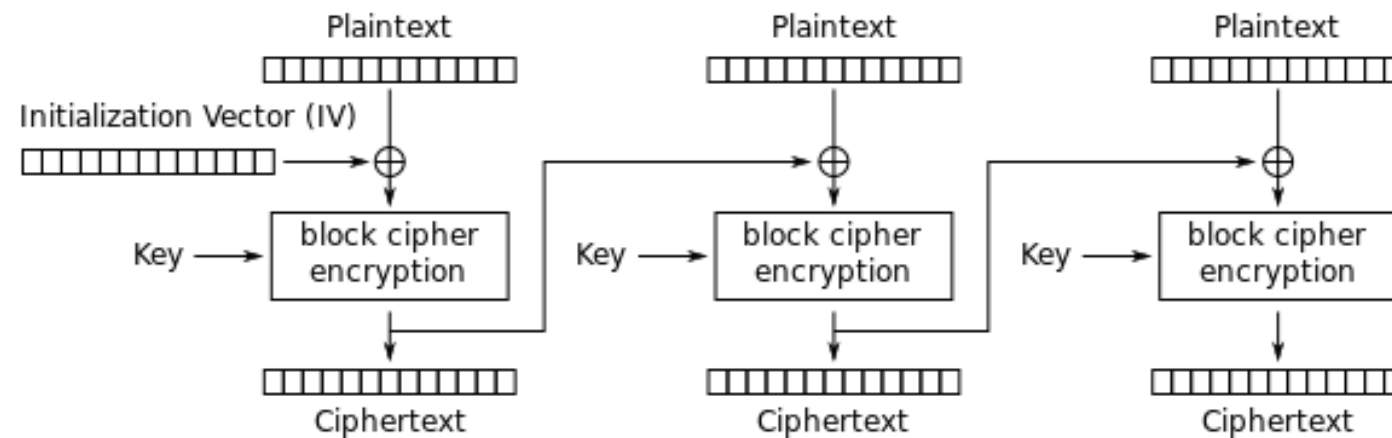
Chosen ciphertext attack

Deduce the plaintext from ciphertext by selecting the ciphertext and acquiring the corresponding plaintext

Adaptive chosen ciphertext attack

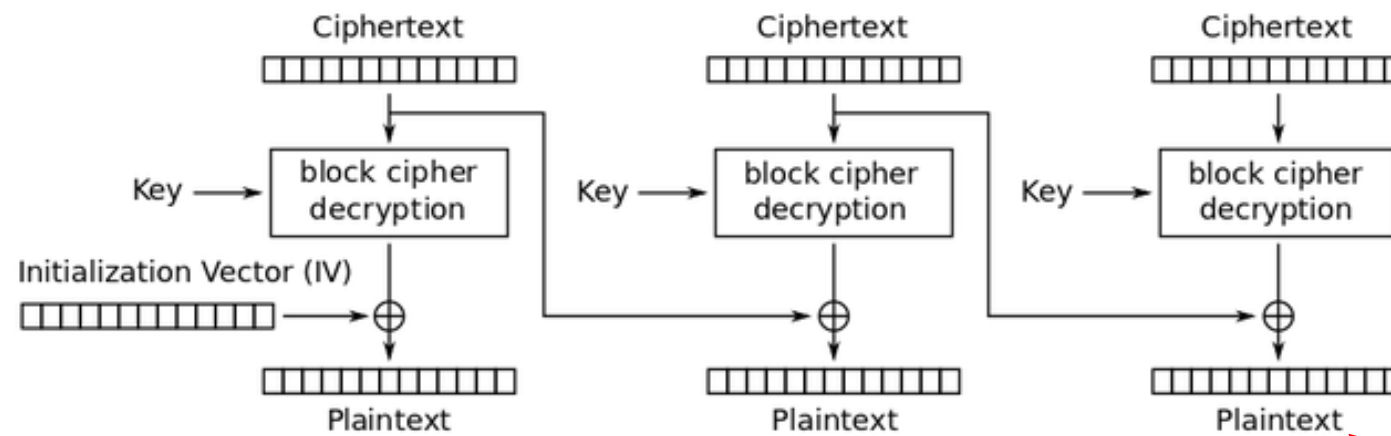
Choose subsequent ciphertexts based on the information received from previous requests

CIPHER BLOCK CHAINING ENCRYPTION



Cipher Block Chaining (CBC) mode encryption

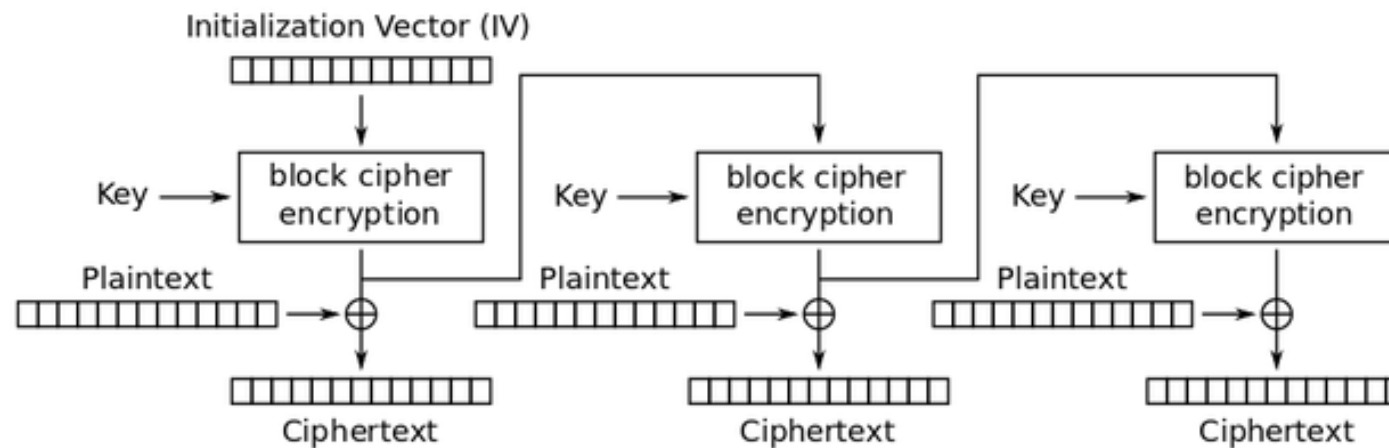
CIPHER BLOCK CHAINING DECRYPTION



Cipher Block Chaining (CBC) mode decryption

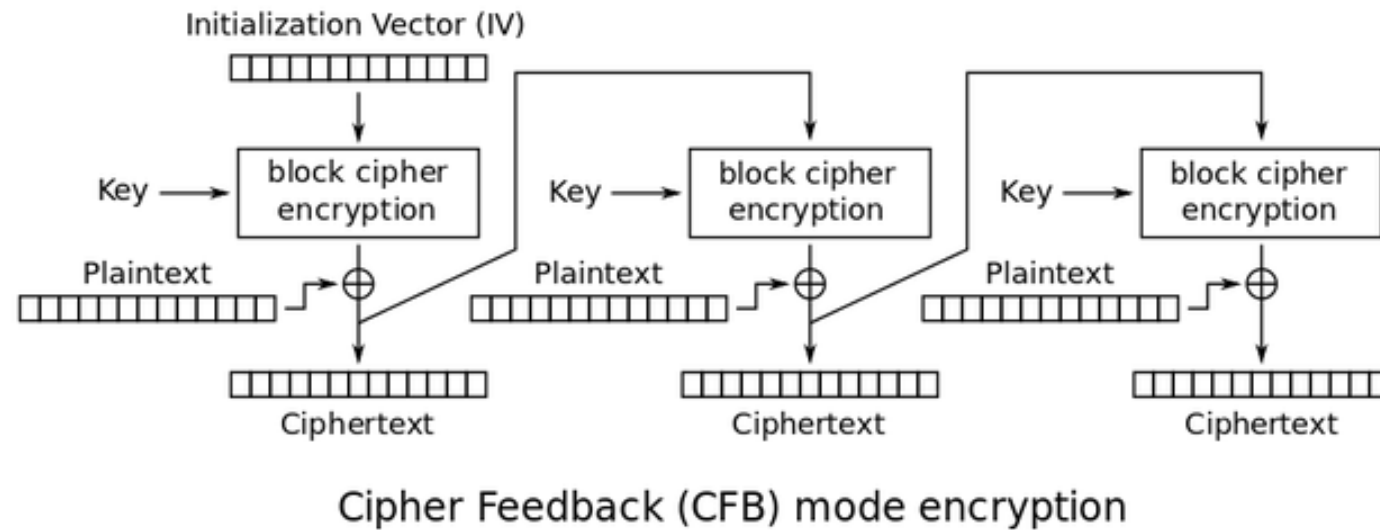
Wenn das "Padding" bekannt ist und das "decryption oracle" auf Padding-Fehler reagiert, kann die Chiffre gebrochen werden, ohne den Schlüssel zu kennen.

OUTPUT FEEDBACK MODE ENCRYPTION

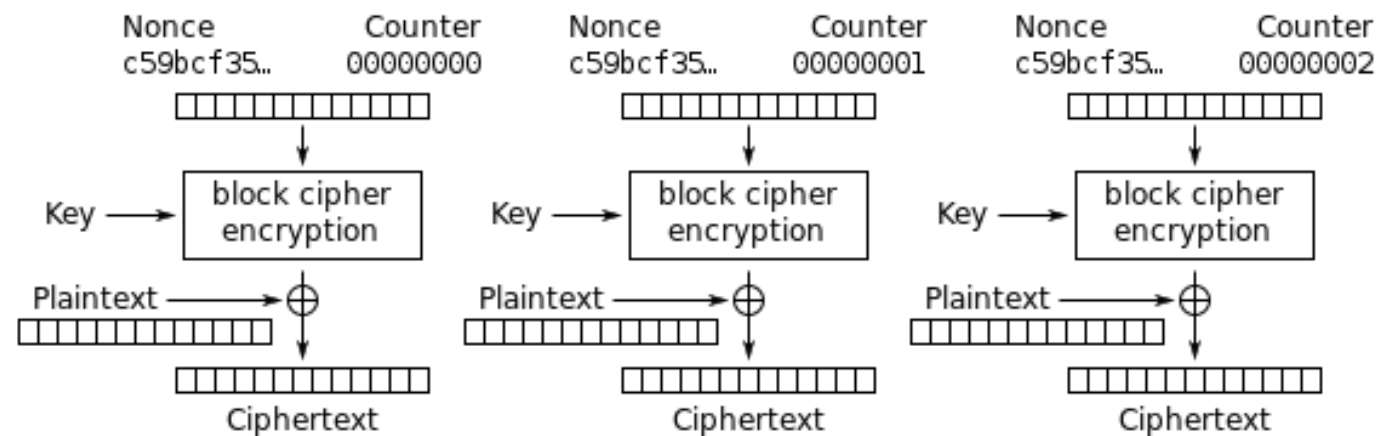


Output Feedback (OFB) mode encryption

CIPHER FEEDBACK MODE ENCRYPTION

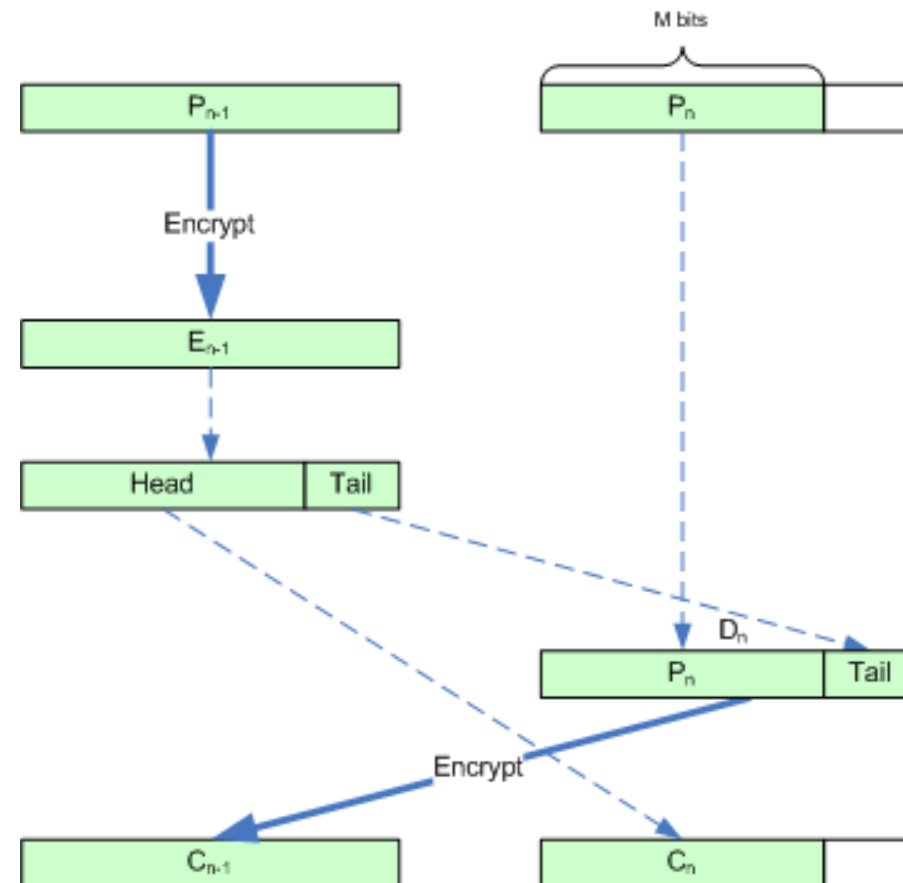


COUNTER MODE ENCRYPTION

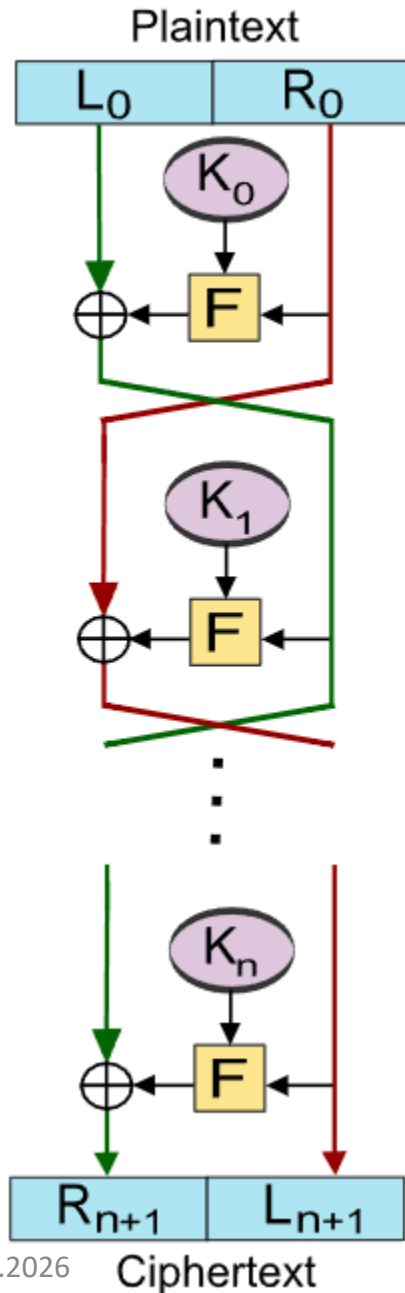


Counter (CTR) mode encryption

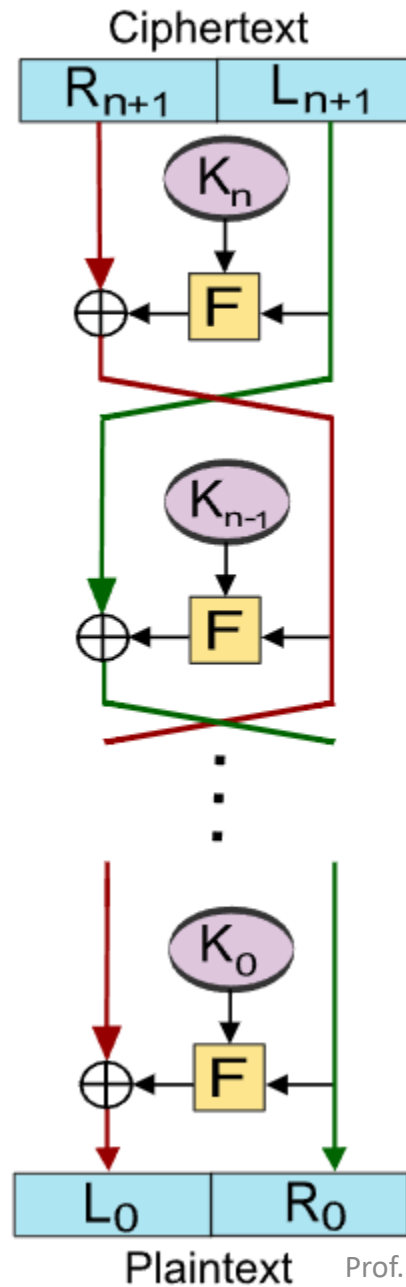
CIPHER TEXT STEALING



Encryption



Decryption



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



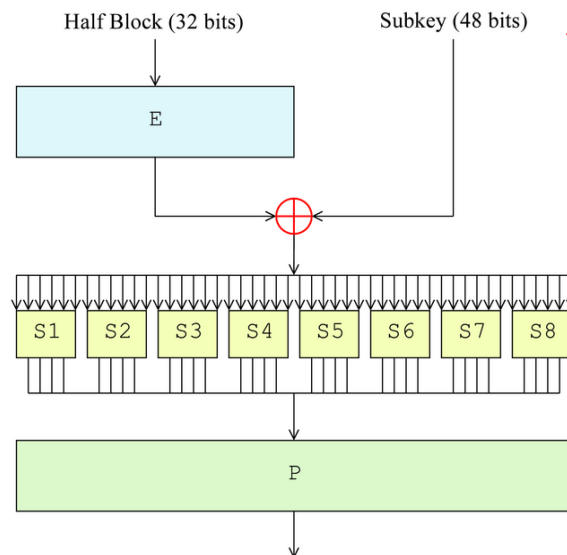
Horst Feistel
1915 - 1990

DATA ENCRYPTION STANDARD (1977)

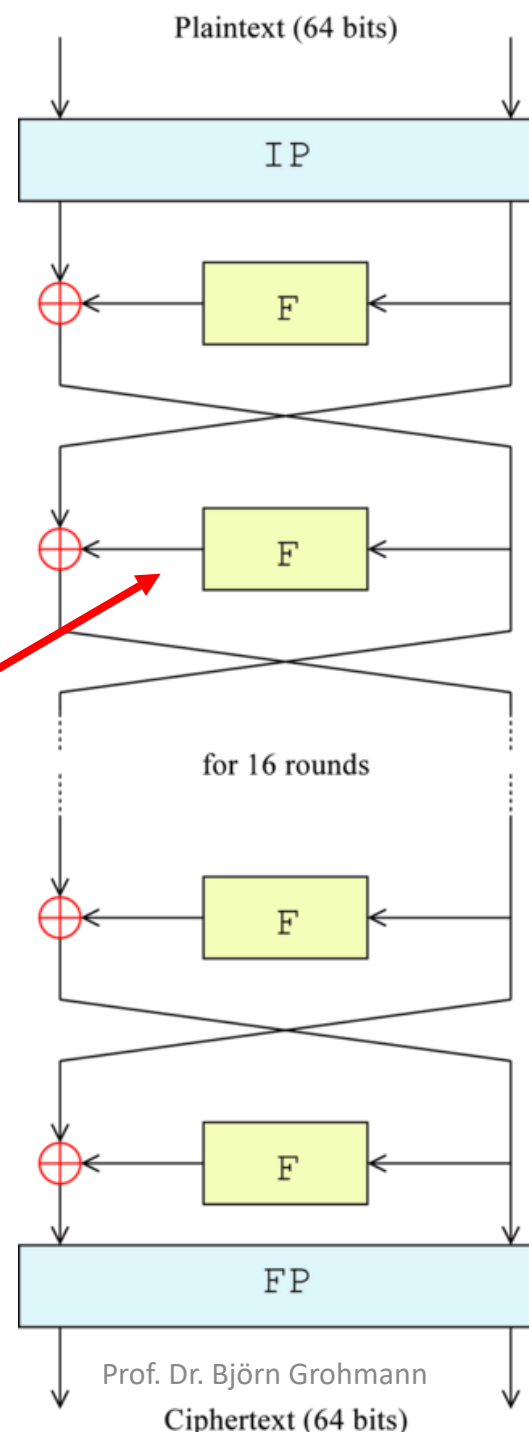


Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

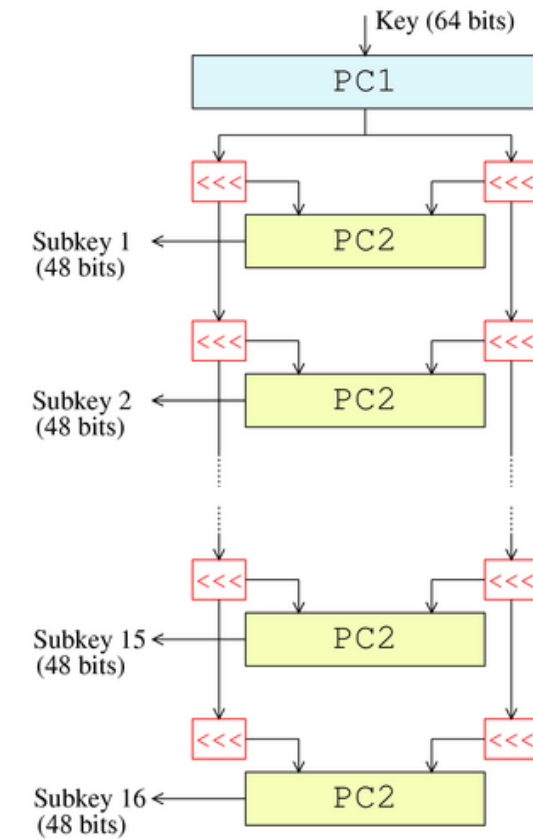
Round function



S-Box



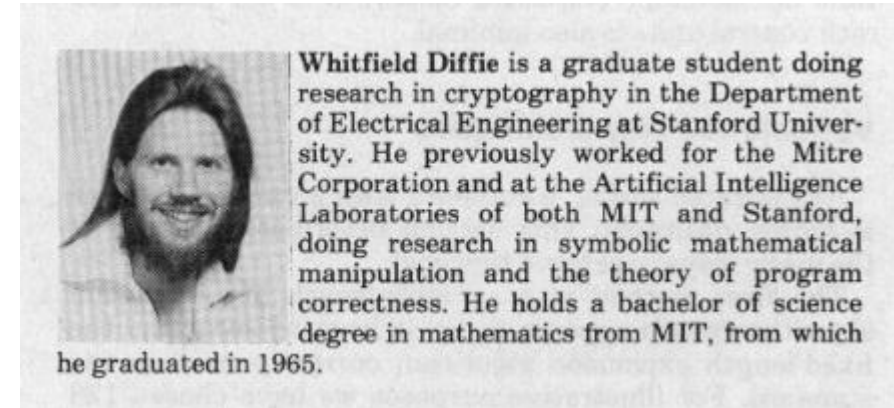
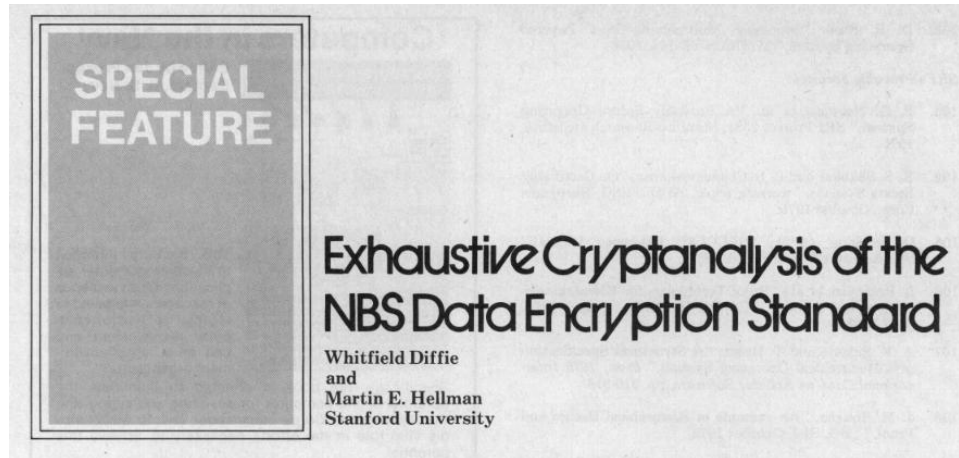
Key Schedule



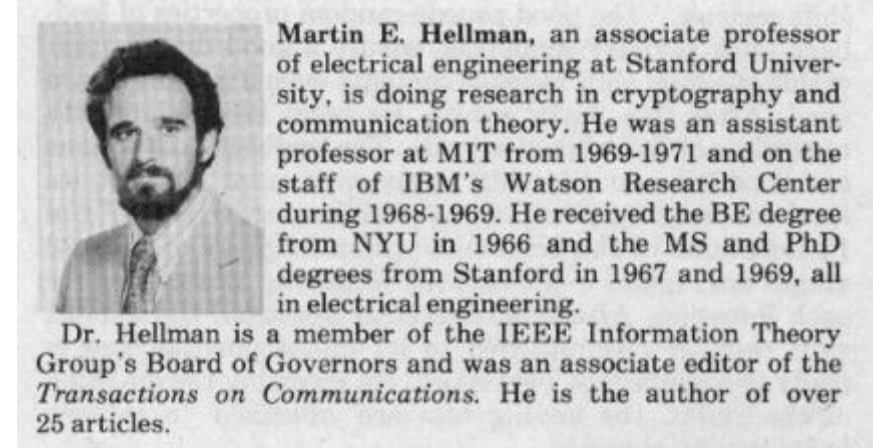
DATA ENCRYPTION STANDARD -- KRITIK



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



In summary, we believe we have made a convincing argument concerning the **insecurity** and planned obsolescence inherent in the proposed cryptostandard. We have also indicated cost-effective ways to avoid the problem. A 128-bit or larger key is needed to preclude exhaustive search and to allow a margin of safety against shortcuts to exhaustive search. We hope that those readers who will be most affected by this standard will let their views be known to NBS. ■



ADVANCED ENCRYPTION STANDARD (2001)



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

**Federal Information
Processing Standards Publication 197**

November 26, 2001

Announcing the ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

ADVANCED ENCRYPTION STANDARD



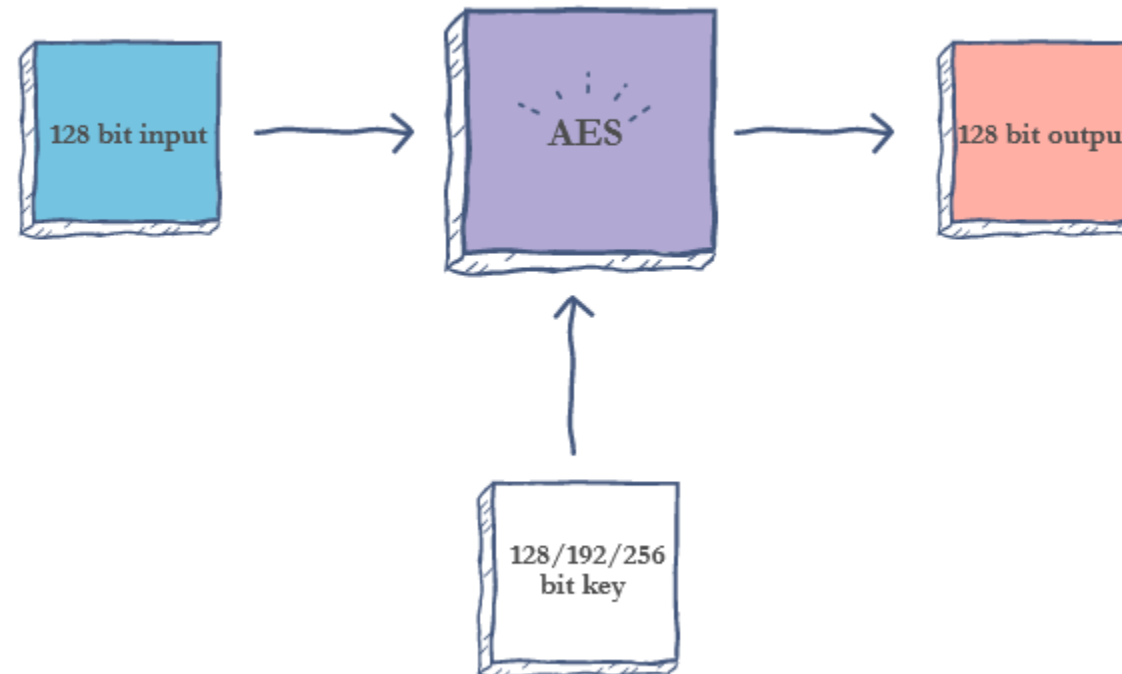
Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

	DES	AES
Developed	1977	2000
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block size	64 bits	128 bits
Key length	56 bits	128/192/256 bits
Security	Rendered insecure	Considered secure

ADVANCED ENCRYPTION STANDARD



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



ADVANCED ENCRYPTION STANDARD 128



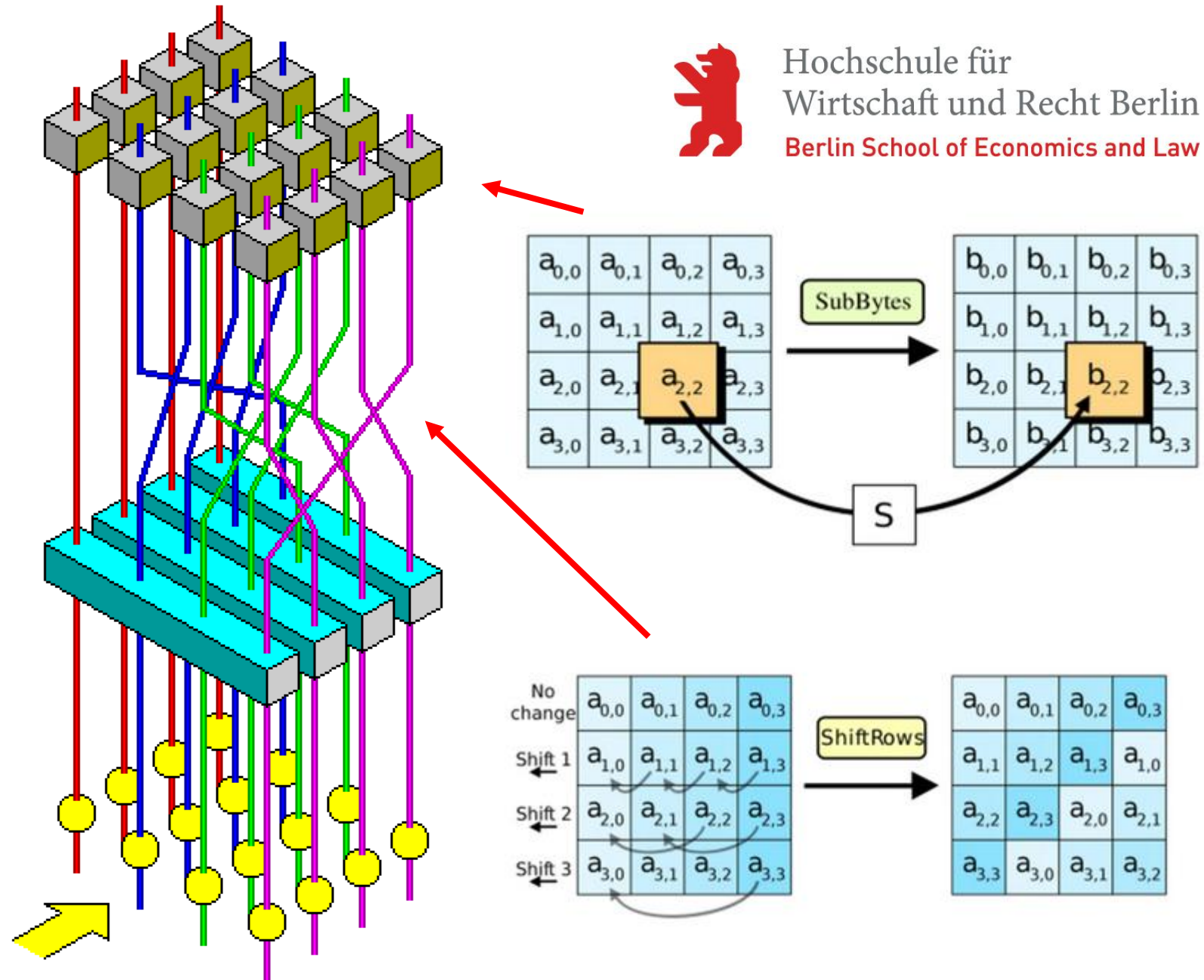
```
function AESK(M)
  (K0, ..., K10) ← expand(K)
  s ← M ⊕ K0
  for r = 1 to 10 do
    s ← S(s)
    s ← shift-rows(s)
    if r ≤ 9 then s ← mix-cols(s) fi
    s ← s ⊕ Kr
  endfor
  return s
```

```
function expand(K)
  K0 ← K
  for i ← 1 to 10 do
    Ki[0] ← Ki-1[0] ⊕ S(Ki-1[3] ≪ 8) ⊕ Ci
    Ki[1] ← Ki-1[1] ⊕ Ki[0]
    Ki[2] ← Ki-1[2] ⊕ Ki[1]
    Ki[3] ← Ki-1[3] ⊕ Ki[2]
  od
  return (K0, ..., K10)
```

ADVANCED ENCRYPTION STANDARD



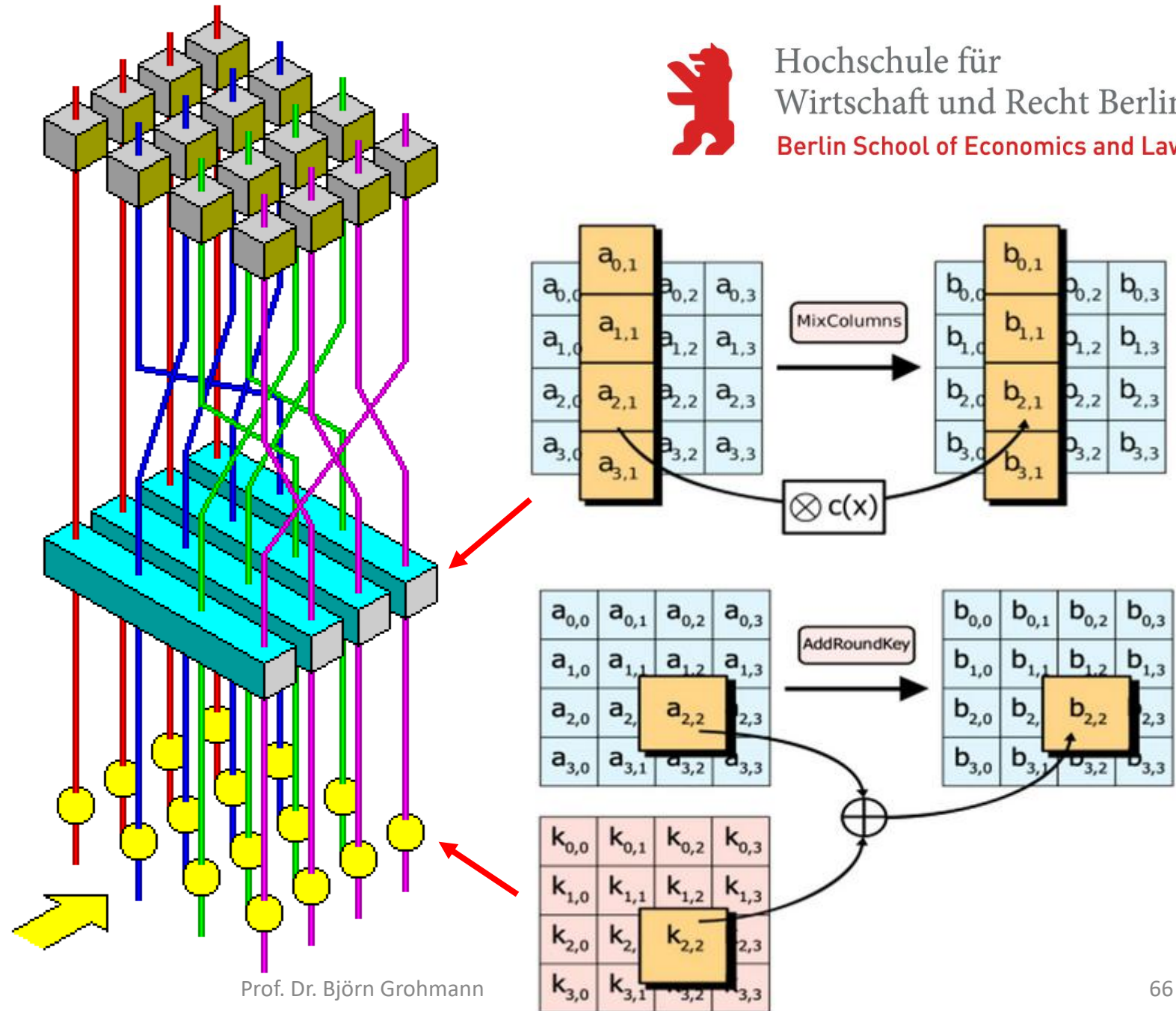
Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



ADVANCED ENCRYPTION STANDARD



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law



ADVANCED ENCRYPTION STANDARD S-BOX



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
60	81	4f	dc	22	2a	90	88	46	ce	b8	14	de	5e	0b	db
e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

ADVANCED ENCRYPTION STANDARD S-BOX



All byte values in the AES algorithm will be presented as the concatenation of its individual bit values (0 or 1) between braces in the order $\{b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0\}$. These bytes are interpreted as finite field elements using a polynomial representation:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{i=0}^7 b_i x^i. \quad (3.1)$$

For example, $\{01100011\}$ identifies the specific finite field element $x^6 + x^5 + x + 1$.

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2 \quad (\text{polynomial notation});$$

$$\{01010111\} \oplus \{10000011\} = \{11010100\} \quad (\text{binary notation});$$

$$\{57\} \oplus \{83\} = \{d4\} \quad (\text{hexadecimal notation}).$$

ADVANCED ENCRYPTION STANDARD S-BOX



In the polynomial representation, multiplication in $GF(2^8)$ (denoted by \bullet) corresponds with the multiplication of polynomials modulo an **irreducible polynomial** of degree 8. A polynomial is irreducible if its only divisors are one and itself. **For the AES algorithm, this irreducible polynomial is**

$$m(x) = x^8 + x^4 + x^3 + x + 1, \quad (4.1)$$

For example, $\{57\} \bullet \{83\} = \{c1\}$, because

$$\begin{aligned} (x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) &= x^{13} + x^{11} + x^9 + x^8 + x^7 + \\ &\quad x^7 + x^5 + x^3 + x^2 + x + \\ &\quad x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

and

$$\begin{aligned} x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \text{ modulo } (x^8 + x^4 + x^3 + x + 1) \\ = x^7 + x^6 + 1. \end{aligned}$$

ADVANCED ENCRYPTION STANDARD S-BOX



Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

The multiplication defined above is associative, and the element $\{01\}$ is the multiplicative identity. For any non-zero binary polynomial $b(x)$ of degree less than 8, the multiplicative inverse of $b(x)$, denoted $b^{-1}(x)$, can be found as follows: the **extended Euclidean algorithm** [7] is used to compute polynomials $a(x)$ and $c(x)$ such that

$$b(x)a(x) + m(x)c(x) = 1. \quad (4.2)$$

It follows that the set of 256 possible byte values, with XOR used as addition and the multiplication defined as above, has the structure of the finite field $GF(2^8)$.

ADVANCED ENCRYPTION STANDARD S-BOX



The **SubBytes ()** transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box). This S-box (Fig. 7), which is invertible, is constructed by composing two transformations:

1. Take the multiplicative inverse in the finite field $GF(2^8)$, described in Sec. 4.2; the element $\{00\}$ is mapped to itself.
2. Apply the following affine transformation (over $GF(2)$):

$$b'_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i \quad (5.1)$$

for $0 \leq i < 8$, where b_i is the i^{th} bit of the byte, and c_i is the i^{th} bit of a byte c with the value $\{63\}$ or $\{01100011\}$. Here and elsewhere, a prime on a variable (e.g., b') indicates that the variable is to be updated with the value on the right.

ADVANCED ENCRYPTION STANDARD S-BOX



$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$