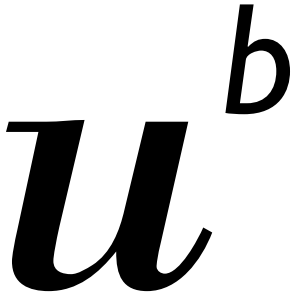


b

UNIVERSITÄT
BERN

UNIVERSITÄT
BERN

Network Security

II. Symmetric Encryption

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 28.02.2022 – 07.03.2022

UNIVERSITÄT BERN

Network Security: Symmetric Encryption

Table of Contents

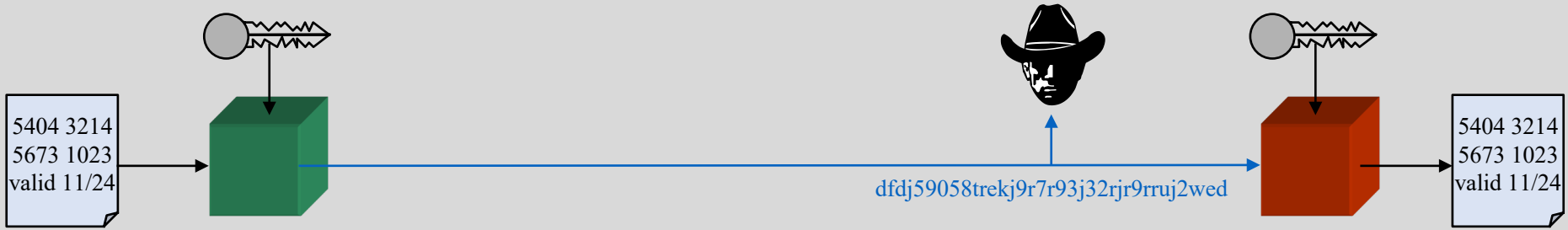
1. Symmetric Encryption Attacks
2. Block and Stream Ciphers
3. Substitution Techniques
4. Advanced Encryption Standard
5. Block Ciphers

UNIVERSITÄT BERN

1. Symmetric Encryption Attacks

1. Symmetric Encryption Operation

- Sender and Receiver exchange common secret key.
- Sender encrypts data with secret key.
- Receiver decrypts data with secret key.
- Example: Advanced Encryption Standard



1. Symmetric Encryption Attacks

2. Cryptanalysis and Brute Force Attacks

Cryptanalysis

Cryptanalytic attacks rely on

- nature of algorithm,
- some knowledge of general plaintext characteristics, and
- some sample plaintext-ciphertext pairs.

Brute Force Attack

Attacker tries every possible key on a piece of ciphertext until intelligible translation into plaintext is obtained.

1. Symmetric Encryption Attacks

3. Attack Models and what is known to attacker

- Ciphertext only
  - encryption algorithm
  - ciphertext to be decoded
- Known plaintext
  - encryption algorithm
  - ciphertext to be decoded
  - pairs of (plaintext, ciphertext)
- Chosen plaintext
  - encryption algorithm
  - ciphertext to be decoded
  - plaintext (chosen by cryptanalyst) + corresponding ciphertext
- Chosen ciphertext
  - encryption algorithm
  - ciphertext to be decoded
  - ciphertext (chosen by cryptanalyst) + corresponding plaintext
- Chosen text
  - encryption algorithm
  - ciphertext to be decoded
  - plaintext + corresponding ciphertext (both can be chosen by cryptanalyst)

1. Symmetric Encryption Attacks

4.1 Chosen Plaintext Attack

Informally:

- An adversary selects two messages m_0, m_1.
- Oracle picks random bit b and encrypts m_b.
- Adversary should not guess b with non-negligible probability.

1. Symmetric Encryption Attacks

4.2 Chosen Plaintext Attack Indistinguishability

CPA indistinguishability experiment $PrivK^{cpa}_{A,\Pi}(n)$:

1. A key k is generated by running $Gen(1^n)$.
2. Adversary A is given input 1^n and oracle access to $Enc_k(\cdot)$, and outputs a pair of messages m_0 and m_1 of the same length.
3. A uniform bit $b \in \{0, 1\}$ is chosen, and then a ciphertext $c \leftarrow Enc_k(m_b)$ is computed and given to A.
4. The adversary A continues to have oracle access to $Enc_k(\cdot)$, and outputs bit b'.
5. The output of the experiment is defined to be 1 if b' = b, 0 otherwise.
   In the former case: "A succeeds".

A private-key encryption scheme Π = (Gen, Enc, Dec) has indistinguishable encryptions under a chosen-plaintext attack, or is CPA-secure, if for all probabilistic polynomial-time adversaries A there is a negligible function negl such that

$$Pr(PrivK^{cpa}_{A,\Pi}(n) = 1) \leq 1/2 + negl(n),$$

where the probability is taken over the randomness used by A, as well as the randomness used in the experiment.

UNIVERSITÄT BERN

2. Block and Stream Ciphers

1. Block Cipher Operation

UNIVERSITÄT BERN

2. Block and Stream Ciphers

2. Substitution and Permutation

Substitution

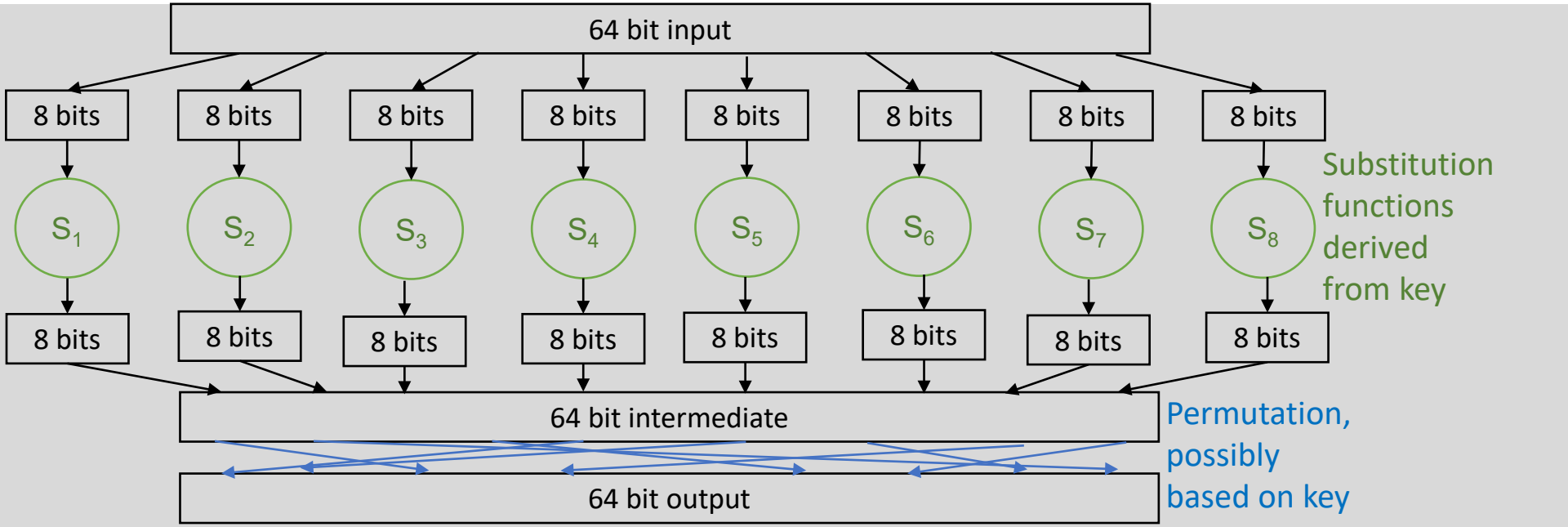
- specifies for each of the 2^k possible values of the input: the k-bit output.
- This would be impractical to build for 64-bit blocks, but would be feasible with blocks of length of 8 bits.
- To specify a completely randomly chosen substitution for k-bit blocks would take about $k \cdot 2^k$ bits.

Permutation

- Specifies for each of the k input bits, the output position to which it goes, e.g.,
  - 1st bit → 13th bit of output
  - 2nd bit → 61st bit of output
  - …
- Specification of a completely randomly chosen permutation of k bits would take $k \cdot \log_2 k$ bits.

2. Block and Stream Ciphers

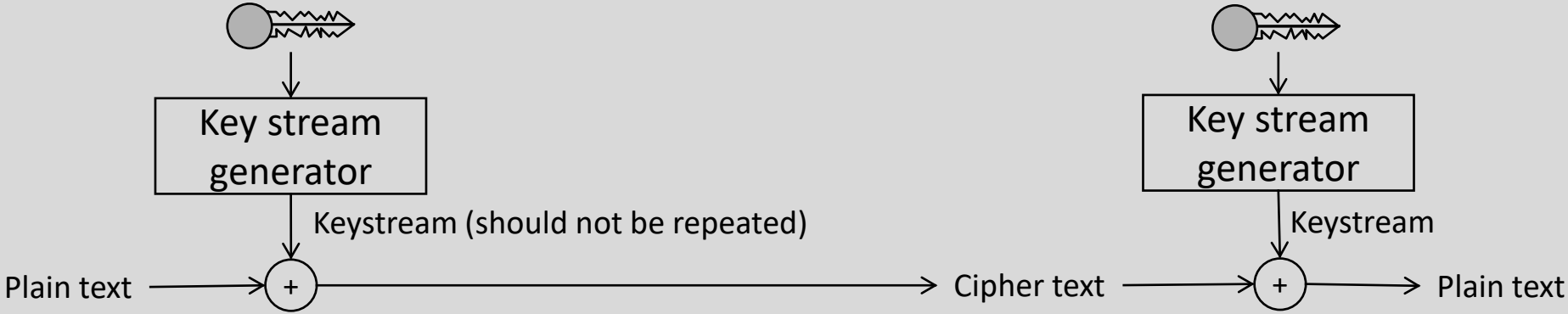
3. Block Cipher Example



UNIVERSITÄT BERN

2. Block and Stream Ciphers

4. Stream Cipher Operation



2. Block and Stream Ciphers

5. Stream Cipher Design Considerations

- Encryption sequence should have a large period.
- Properties of true random number generation, e.g., equal 0 and 1 bits
- Long keys

UNIVERSITÄT BERN

3. Substitution Techniques

1. Caesar Cipher

- Each letter is replaced by the letter k places away.
- C = E(k, p) = (p + k) mod 26
- p = D(k, C) = (C - k) mod 26
- k = 3:
  - Plain: abcdefghijklmnopqrstuvwyxz
  - Cipher: defghijklmnopqrstuvwyxzabc
- Example
  - Plaintext: meet me after the toga party
  - Ciphertext: phhw ph diwhu wkh wrjd sduwb
- Brute-Force Attack (25 keys !)

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

3. Substitution Techniques

2. Monoalphabetic Ciphers

Permutations

- Finite set of elements with each element appears exactly once.
- {a, b, c}: 6 = 3! permutations: abc, acb, bac, bca, cab, cba
- In general: n! permutations for a set of n elements

If the cipher line (cf. Caesar cipher) can contain any permutation, then there are $26! > 4 \cdot 10^{26}$ keys

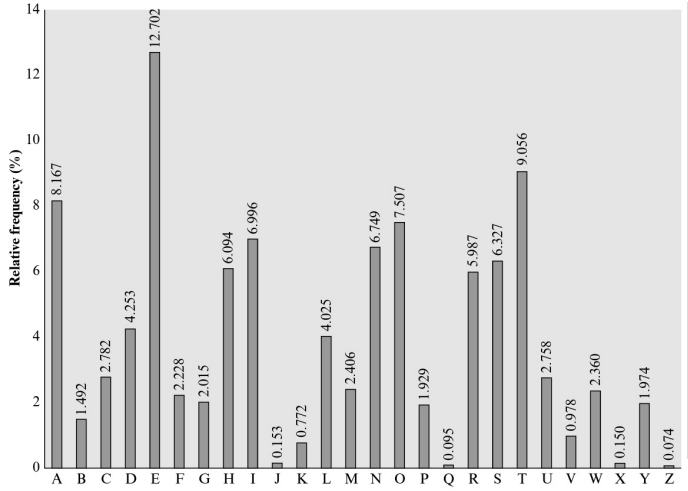
UNIVERSITÄT BERN

3. Substitution Techniques

2.1 Monoalphabetic Ciphers: Cryptanalysis

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

- P and Z are probably equivalent to e and t.
- {S, U, O, M, H} have high frequencies and probably correspond to letters from {a, h, i, n, o, r, s}.
- {A, B, G, Y, I, J} have low frequencies and probably correspond to {b, j, k, q, v, x, z}.
- Most common digram is ZW → th, P → e



3. Substitution Techniques

2.2 Monoalphabetic Ciphers: Cryptanalysis

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a         e   e te   a that e e a         a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t    ta t ha e ee   a e   th     t   a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e   e e tat   e    the    t
```

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

UNIVERSITÄT BERN

3. Substitution Techniques

3. Multiple Letter Ciphers: Playfair

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

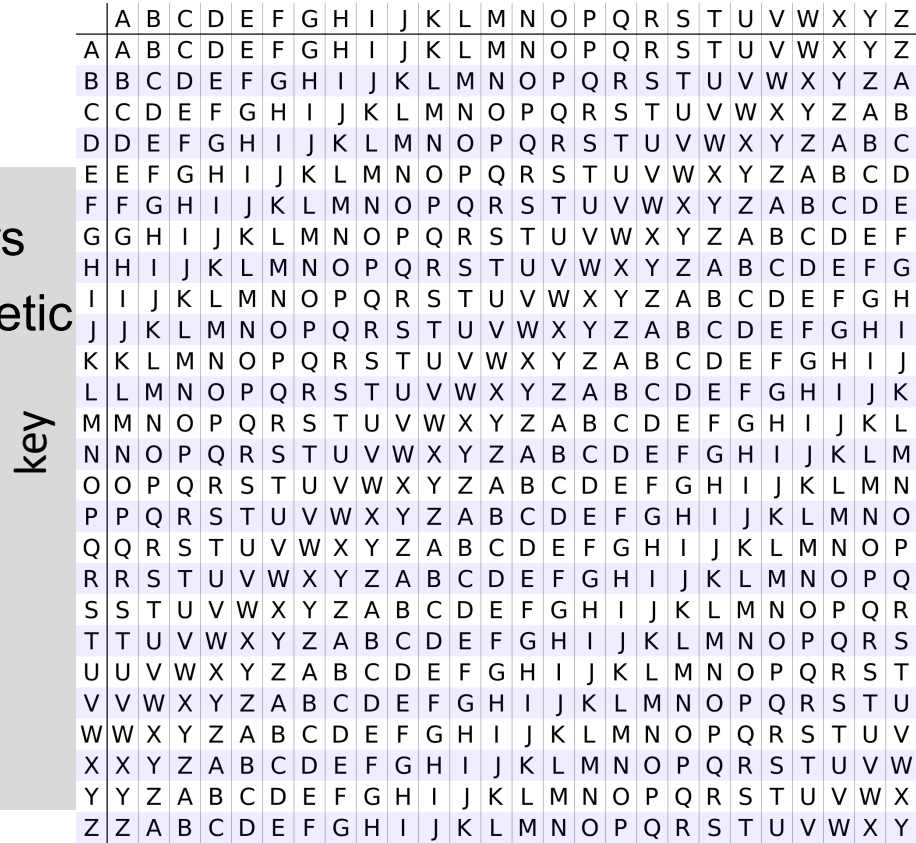
- Use of a 5 x 5 matrix, e.g., for keyword monarchy
- Encryption of letter pairs, 26 x 26 = 676 digrams.
- Encryption rules
  1. Repeating letters in the same pair are separated by a filler letter, e.g., ba lx lo on
  2. 2 plaintext letters in the same row are each replaced by the letter to the right, e.g., ar → RM
  3. 2 plaintext letters in the same column are each replaced by the letter beneath, e.g., mu → CM
  4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter, e.g., hs → BP, ea → JM

UNIVERSITÄT BERN

3. Substitution Techniques

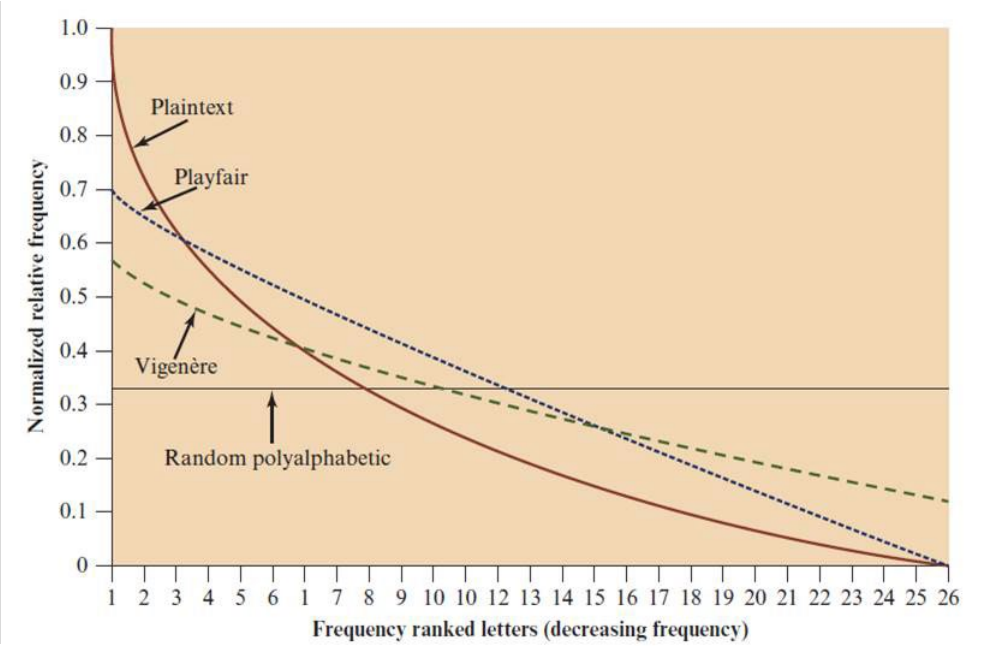
4. Polyalphabetic Ciphers

- Use of several monoalphabetic ciphers
- A key determines which mono-alphabetic substitution rule is used.
- Vigenere cipher consists of 26 Caesar ciphers with shifts 0-25.
- Plaintext: ATTACKATDAWN
- Key: LEMONLEMONLE
- Ciphertext: LXFOPVEFRNHR



3. Substitution Techniques

5. Relative Occurrence of Letters



3. Substitution Techniques

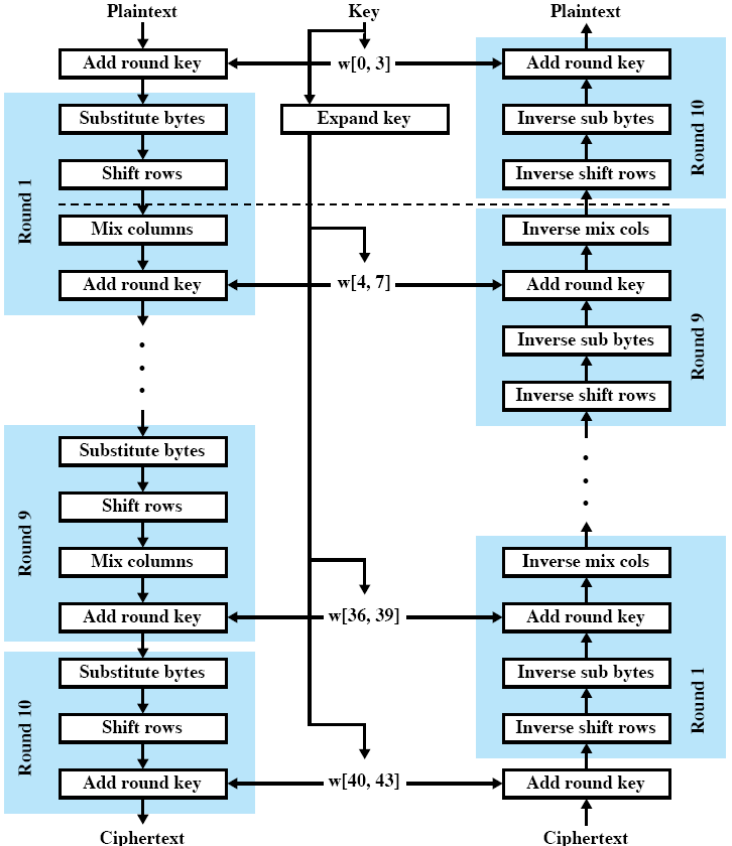
6. One-Time Pads

- One-time use of random key as long as message
- Perfect security
- Problems:
  - Making large quantities of truly random keys
  - Key distribution

4. Advanced Encryption Standard

1. Overview

Encryption

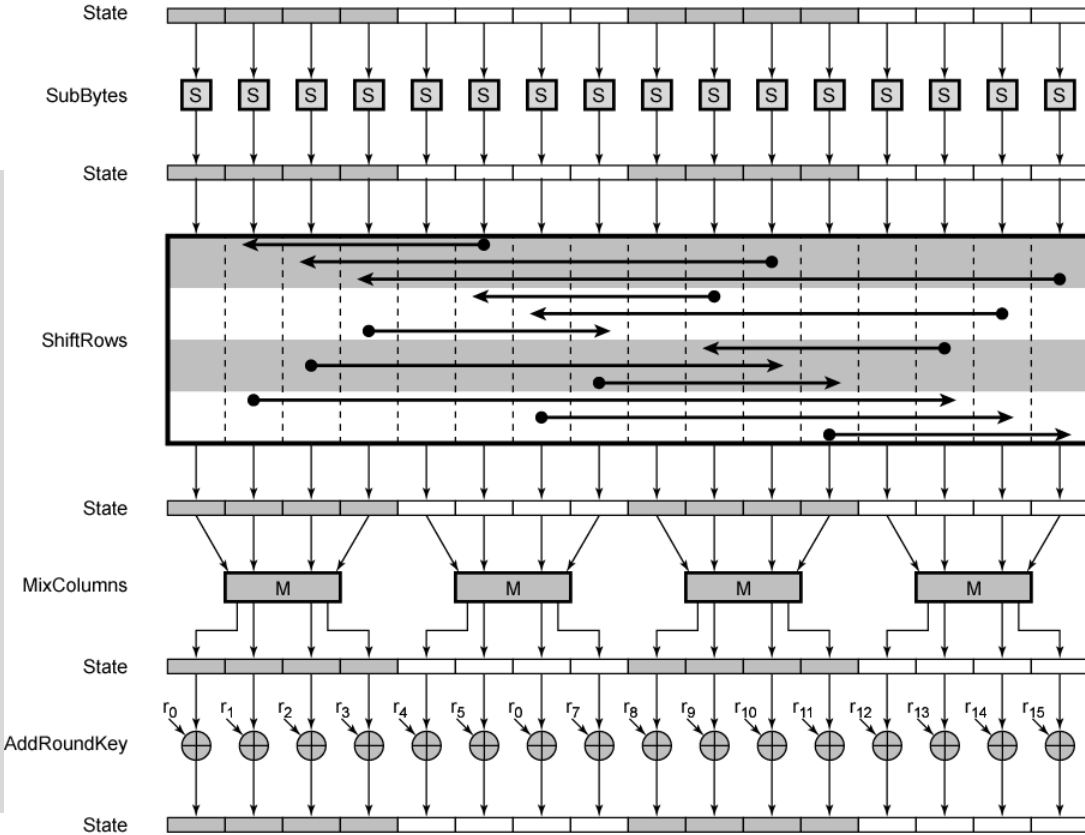


Decryption

UNIVERSITÄT BERN

4. Advanced Encryption Standard

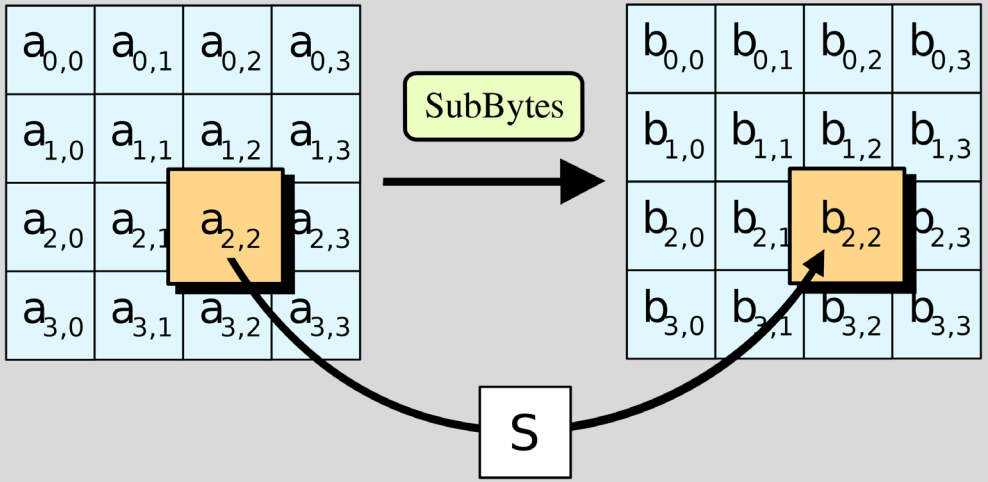
2. Encryption Round



UNIVERSITÄT BERN

4. Advanced Encryption Standard

3. Substitute Bytes

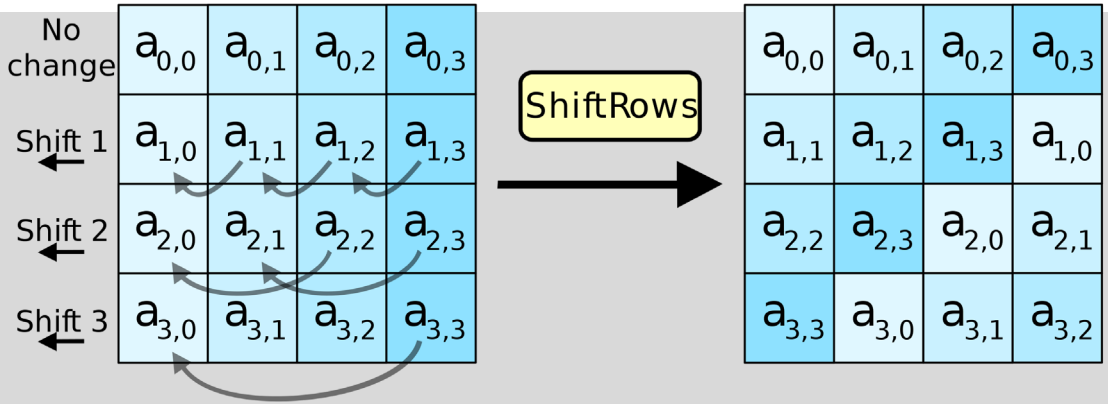


	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

S-Box

4. Advanced Encryption Standard

4. Shift Rows

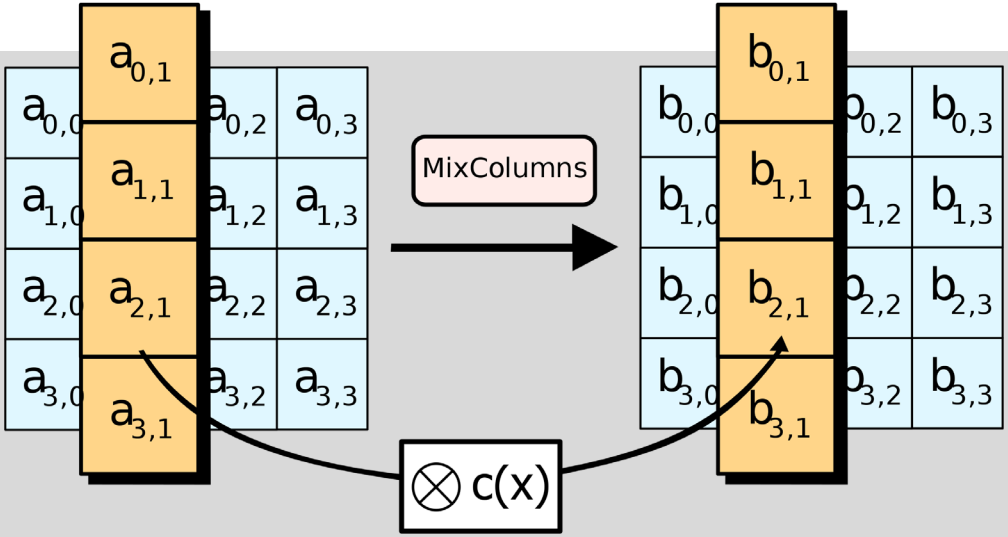


1. Row: no change
2. Row: 1 byte circular shift
3. Row: 2 byte circular shift
4. Row: 3 byte circular shift

UNIVERSITÄT BERN

4. Advanced Encryption Standard

5. Mix Columns



$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Forward matrix

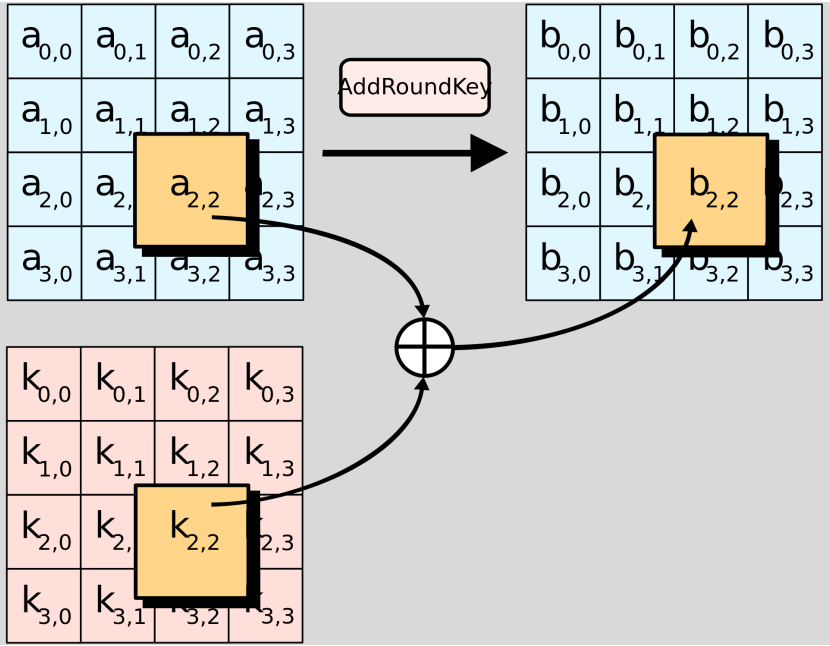
Inverse matrix

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

UNIVERSITÄT BERN

4. Advanced Encryption Standard

6. Add Round Key



UNIVERSITÄT BERN

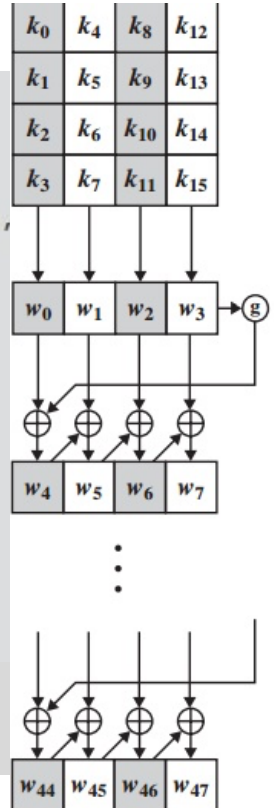
4. Advanced Encryption Standard

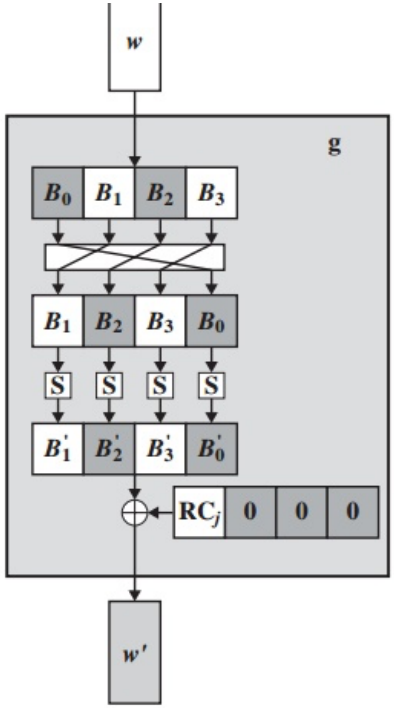
7. Key Expansion

```
KeyExpansion (byte key[16], word w[44])
{
    word temp
    for (i = 0; i < 4; i++)    w[i] = (key[4*i], key[4*i+1],
                                       key[4*i+2],
                                       key[4*i+3]);

    for (i = 4; i < 44; i++)
    {
     temp = w[i - 1];
     if (i mod 4 = 0)    temp = SubWord (RotWord (temp))
                                ⊕ Rcon[i/4];

     w[i] = w[i-4] ⊕ temp
    }
}
```





(b) Function g

5. Block Ciphers

Design Criteria

- Overhead
- Error recovery and propagation
- Diffusion
  - how plaintext statistics are reflected in ciphertext
- Security
  - whether ciphertext blocks leak information about plaintext blocks

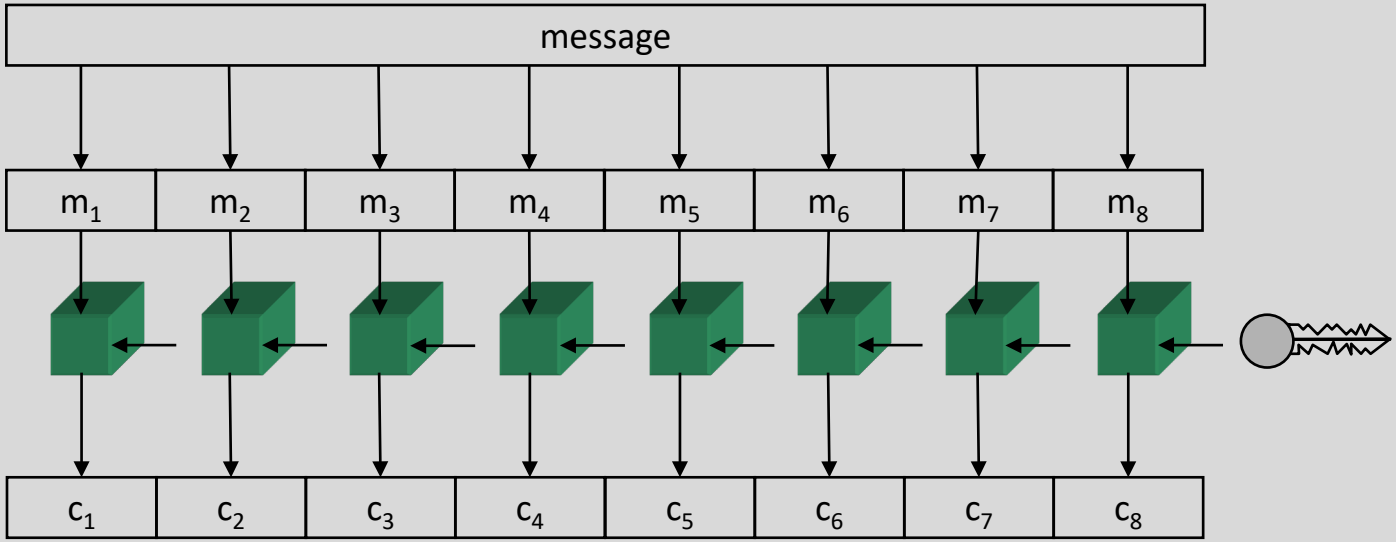
Modes of Operation

1. Electronic Code Book
   - Secure transmission of single values
2. Cipher Block Chaining
   - General purpose block transmissions
   - Authentication
3. Cipher FeedBack Mode
   - General purpose stream transmission
   - Authentication
4. Output Feedback Mode
   - Stream-oriented transmission over noisy channels
5. CounTeR Mode
   - General purpose, high-speed block transmissions

UNIVERSITÄT BERN

5. Block Ciphers

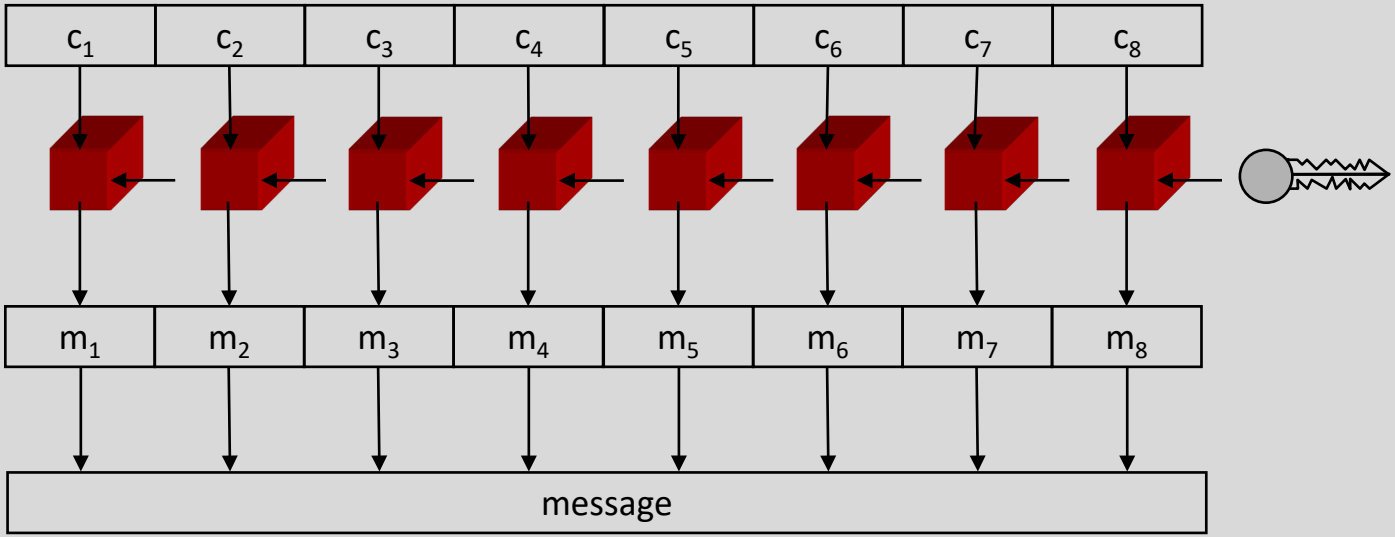
1.1 Electronic Code Book Encryption



UNIVERSITÄT BERN

5. Block Ciphers

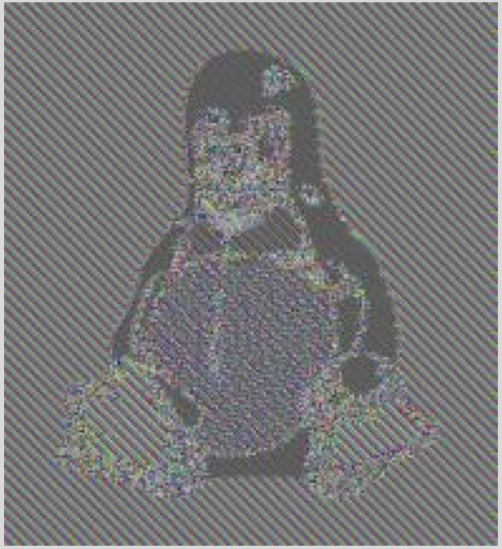
1.2 Electronic Code Book Decryption



5. Block Ciphers

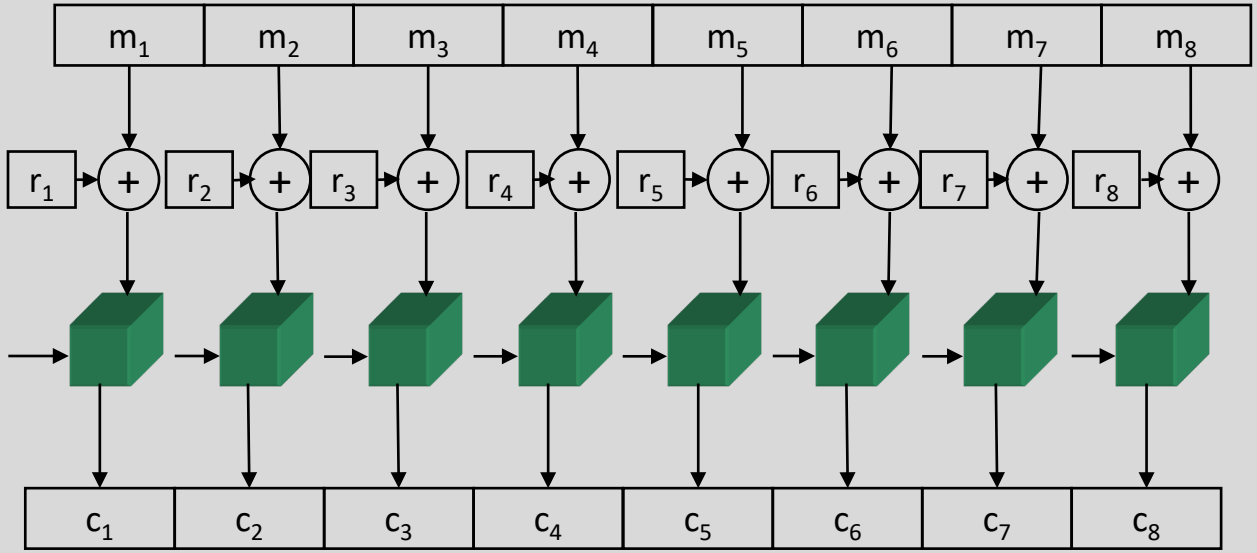
1.3 Electronic Code Book Problems

- If a message has two identical blocks: The corresponding two blocks of ciphertext are also identical.
- This will give the eavesdropper at least some information, which is useful depending on the context.



5. Block Ciphers

1.4 Randomized Electronic Code Book Encryption

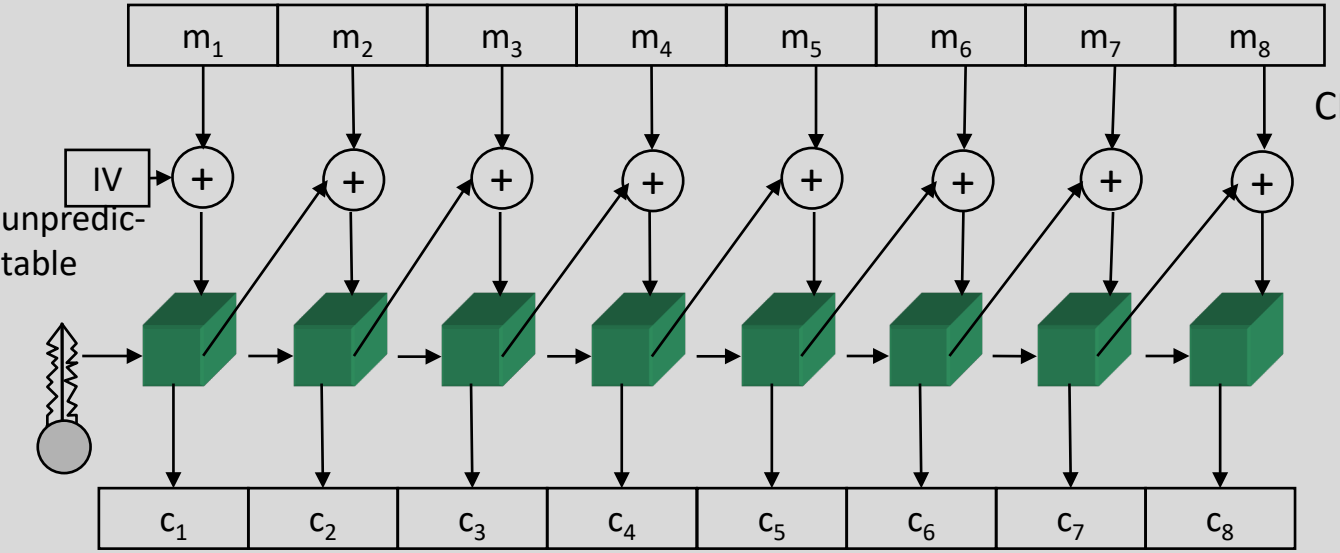


- Low efficiency due to random number transmission
- Attacker can rearrange blocks.

UNIVERSITÄT BERN

5. Block Ciphers

2.1 Cipher Block Chaining Encryption



CRC to protect from modifications

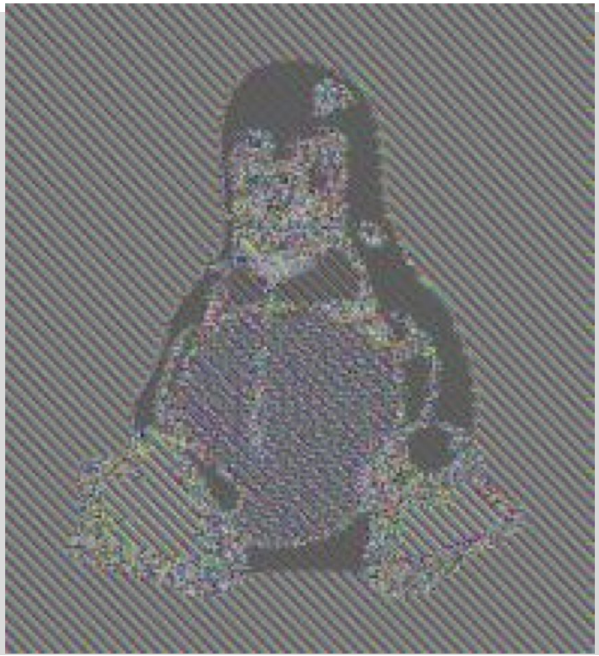
5. Block Ciphers

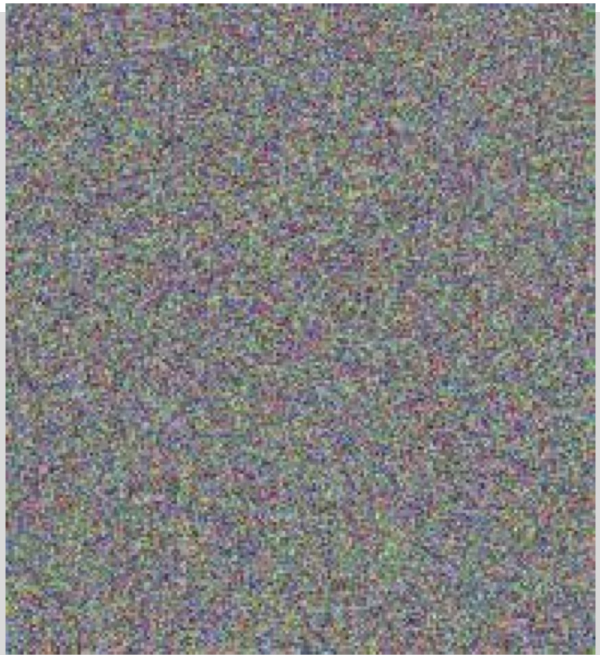
2.2 Cipher Block Chaining Problems

- Reception of a block, e.g. 64 bits, required before block can be decrypted.
- 1 bit error has impact on whole block.

5. Block Ciphers

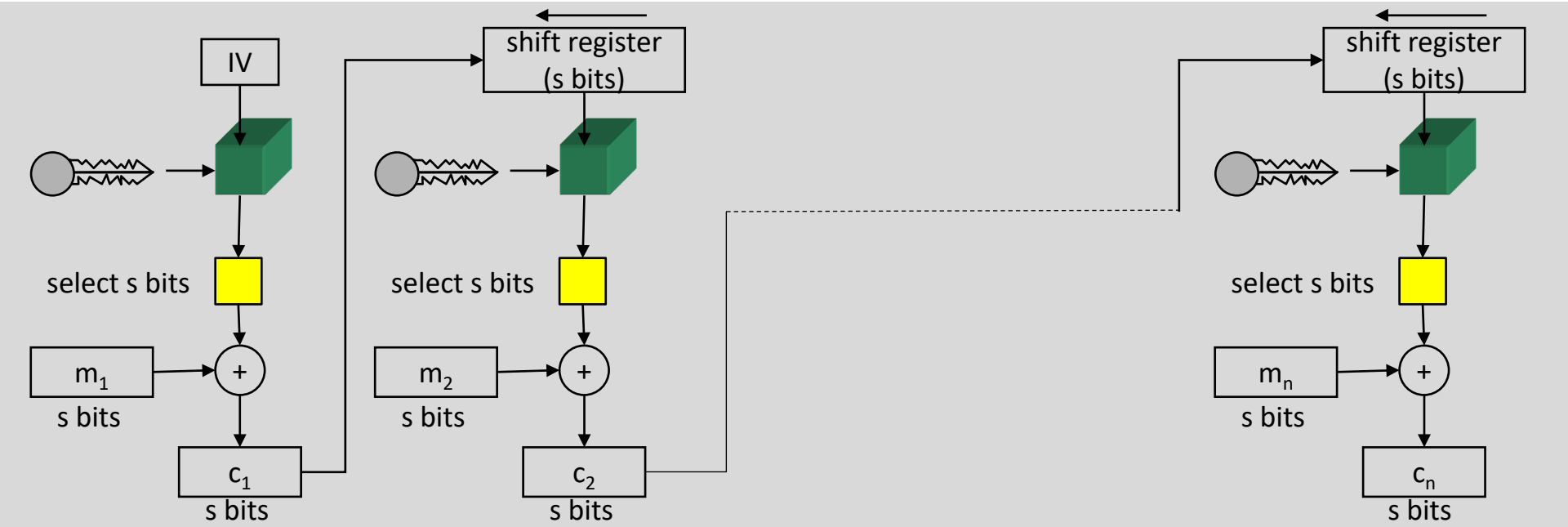
2.3 ECB vs CBC





5. Block Ciphers

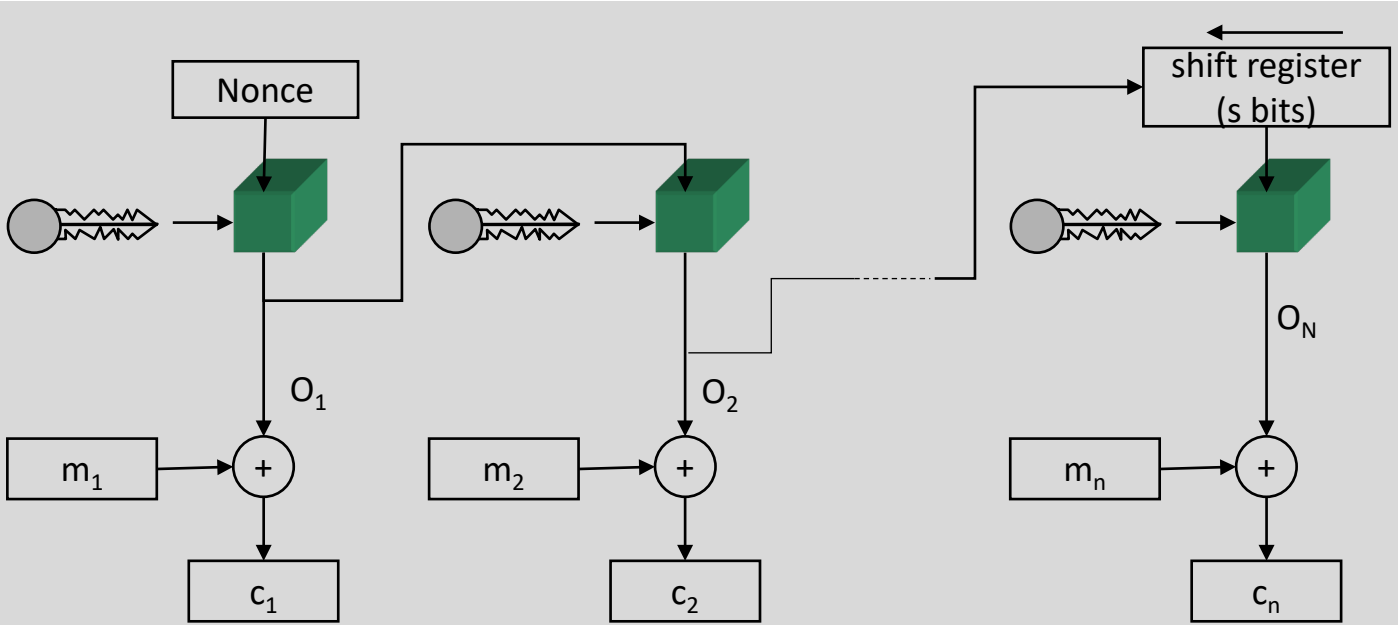
3. Cipher FeedBack Mode



UNIVERSITÄT BERN

5. Block Ciphers

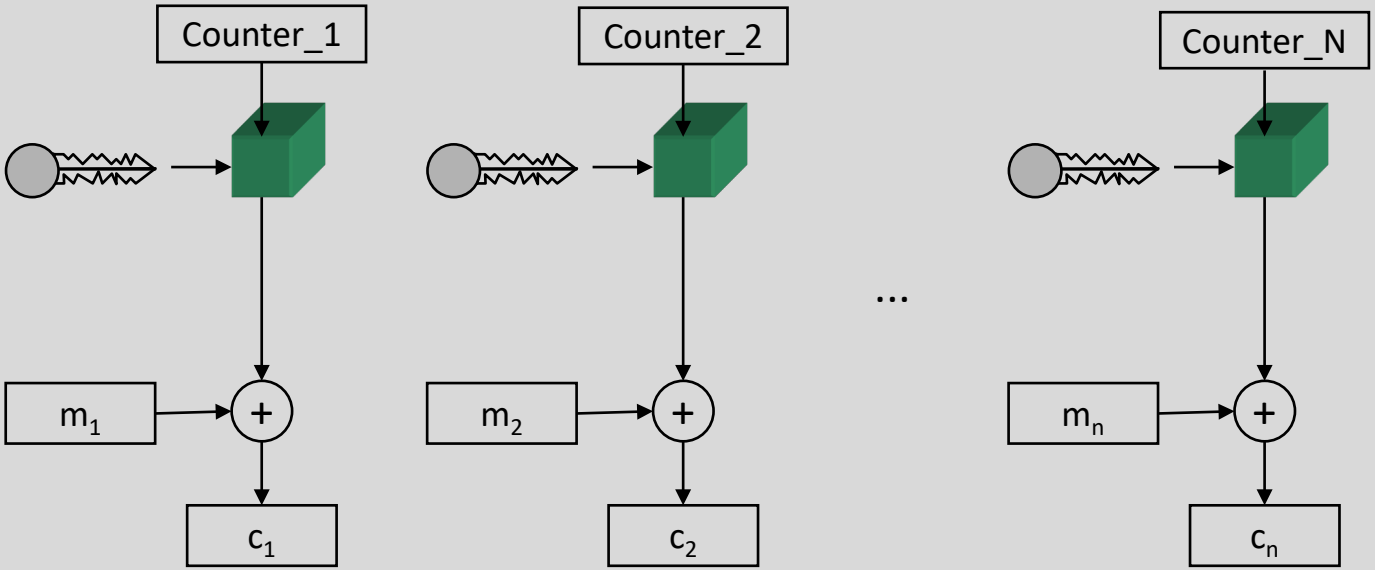
4. Output FeedBack Mode



+ no propagation of bit errors !
- more vulnerable to message stream modification attack than CFB

5. Block Ciphers

5. CounTeR Mode



Counter_N+1 = Counter_N + 1

+ hardware efficiency
+ software efficiency
+ random access
+ security
+ simplicity

Thanks

for Your Attention

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 28.02.2022 – 07.03.2022