

Ivana.Budinska@savba.sk

Na čo nám je šifrovanie?



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

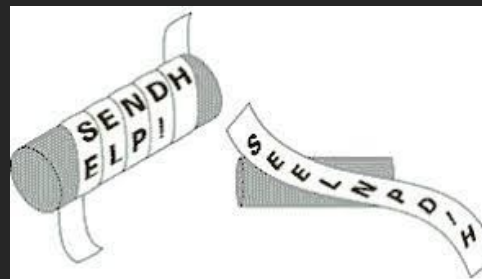


História

- cca 1900p.n.l. - egyptské hieroglyfy- použitie neštandardných symbolov



- 1500p.n.l. – Mezopotámia – substitučná šifra na základe zvukovej zhody v rôznych slovách (formula na výrobu keramiky)
- 600-500p.n.l. – hebrejci – substitučné šifry: atbaš, albam, atbah
- 500p.n.l. – grécko a Sparta – mechanický šifra – skytalé



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED



História

- 360 p.n.l. – AINEIAS TAKTIKOS – 16 šifrovacích metód, napr. nahradenie písmen číslami
- 300 p.n.l. – India – substitúcia znakov podľa zvukovej príbuznosti
- 60- 50p.n.l. – Julius Caesar – Cézarova šifra – každé písmeno sa nahradí písmenom, nasledujúcim 3 písmená za ním
- 1379 – nomenklátory (Gabriel de Lavinde pre vzdor pápeža Klementa VIII.): úplná substitučná abeceda, dvoj písmenkové kódy pre najfrekventovanejšie slová a „klamače“.

1400 – 1407 – Leon Batista Alberti – otec západnej kryptografie.

- Roztriedenie systémov šifrovania na substitúciu a transpozíciu, objav polyalfabetickej substitúcie a šifrovanie kódov
- Zostrojil šifrovací disk (kotúče reprezentujúce otvorené a zašifrované znaky, ich otáčanie simuluje polyalfabetickú substitúciu)



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED



História – Vigenère

- 1586 – šifrovanie pomocou šifrovacieho kľúča

Správa: k r y p t o l o g i a

Kľúč: b o d

k	y	b	e	r	n	e	t	i	k	a
b	o	d	b	o	d	b	o	d	b	c
L	M	E	F	F	Q	F	H	L	L	C

	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

História – Vigenère

- 1586 – šifrovanie pomocou šifrovacieho kľúča

Správa: k r y p t o l o g i a

Kľúč: b o d

k	y	b	e	r	n	e	t	i	k	a
b	o	d	b	o	d	b	o	d	b	o
L	M	E	F	F	Q	F	H	L	L	O



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

História – Vigenère

- 1586 – šifrovanie pomocou šifrovacieho kľúča

Správa: k r y p t o l o g i a

Kľúč: b o d

k	y	b	e	r	n	e	t	i	k	a
b	o	d	b	o	d	b	o	d	b	o
L	M	E	F	F	Q	F	H	L	L	O

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

História – Vigenère

- 1586 – šifrovanie pomocou šifrovacieho kľúča

Správa: k r y p t o l o g i a

Kľúč: b o d

k	y	b	e	r	n	e	t	i	k	a
b	o	d	b	o	d	b	o	d	b	o
L	M	E	F	F	Q	F	H	L	L	O

	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

História – Vigenère

- 1586 – šifrovanie pomocou šifrovacieho kľúča

Správa: k r y p t o l o g i a

Kľúč: b o d

k	y	b	e	r	n	e	t	i	k	a
b	o	d	b	o	d	b	o	d	b	o
L	M	E	F	F	Q	F	H	L	L	O

	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

História – Vigenère

- 1586 – šifrovanie pomocou šifrovacieho kľúča

Správa: k r y p t o l o g i a

Kľúč: b o d

k	y	b	e	r	n	e	t	i	k	a
b	o	d	b	o	d	b	o	d	b	o
L	M	E	F	F	Q	F	H	L	L	O



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

	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

História – Vigenère

- 1586 – šifrovanie pomocou šifrovacieho kľúča

Správa: k r y p t o l o g i a

Kľúč: b o d

k	y	b	e	r	n	e	t	i	k	a
b	o	d	b	o	d	b	o	d	b	o
L	M	E	F	F	Q	F	H	L	L	O



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

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

Mechanické a elektronické šifrovacie stroje

- 1790 – Jeffersonov valec – 26 rovnakých koliesok na spoločnej osi.
- 1860 – Wadsworthov šifrátor – vonkajší a vnútorné koliesko spojené ozubenými kolesami 26/33 zubov. Vodiace okienko ukáže požadované písmeno, vo vonkajšom okienku sa prečíta šifrovaný text.
- 1867 – Wheatstone – podobne, ale používal ručičky (hodinové)
- 1843 – Edgar Allan Poe – Ak vieme niečo zašifrovať, dokážeme to aj odšifrovať - základná otázka kryptografie – bezpečnosť šifier

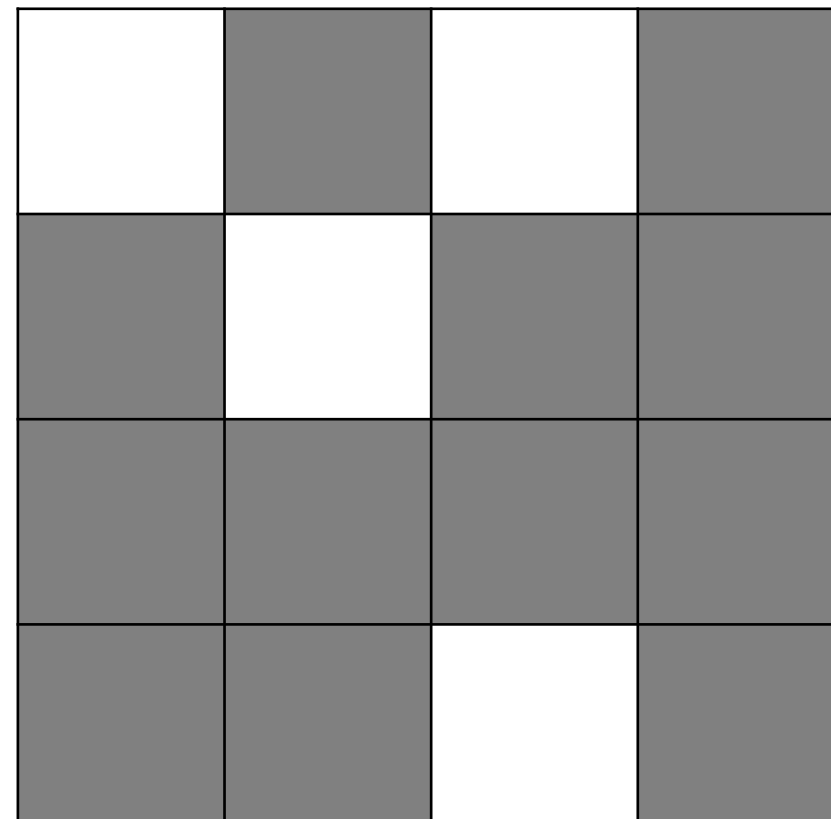


Mechanické a elektronické šifrovacie stroje

- 1881 – Fleisner von Wostrowitz – mechanická pomôcka
- Vo štvorci $n \times n$ políčok sa vystrihne $n \times n/4$ políčok tak, aby pri postupnom otáčaní o 90 stupňov otvory ukazovali vždy na iné políčka.
- Políčka sa postupne zaplňajú. Šifrovaný text sa vypisuje po riadkoch.
- Jules Verne – Nový gróf Monte Cristo,
- Nemecká armáda v I. sv. vojne – poľná šifra



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED



Mechanické a elektronické šifrovacie stroje

- 1881 – Fleisner von Wostrowitz – mechanická pomôcka
- Vo štvorci $n \times n$ políčok sa vystrihne $n \times n/4$ políčok tak, aby pri postupnom otáčaní o 90 stupňov otvory ukazovali vždy na iné políčka.
- Políčka sa postupne zaplňajú. Šifrovaný text sa vypisuje po riadkoch.
- Jules Verne – Nový gróf Monte Christo,
- Nemecká armáda v I. sv. vojne – poľná šifra

Sifrovanie ta bavi



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

S		I	
	F		
		R	

Mechanické a elektronické šifrovacie stroje

- 1881 – Fleisner von Wostrowitz – mechanická pomôcka
- Vo štvorci $n \times n$ políček sa vystrihne $n \times n/4$ políček tak, aby pri postupnom otáčaní o 90 stupňov otvory ukazovali vždy na iné políčka.
- Políčka sa postupne zaplňajú. Šifrovaný text sa vypisuje po riadkoch.
- Jules Verne – Nový gróf Monte Christo,
- Nemecká armáda v I. sv. vojne – poľná šifra

Sifrovanie ta bavi



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

			O
		V	
A			N

Mechanické a elektronické šifrovacie stroje

- 1881 – Fleisner von Wostrowitz – mechanická pomôcka
- Vo štvorci $n \times n$ políčok sa vystrihne $n \times n/4$ políčok tak, aby pri postupnom otáčaní o 90 stupňov otvory ukazovali vždy na iné políčka.
- Políčka sa postupne zaplňajú. Šifrovaný text sa vypisuje po riadkoch.
- Jules Verne – Nový gróf Monte Christo,
- Nemecká armáda v I. sv. vojne – poľná šifra

Sifrovanie ta bavi



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

	I		
		E	
	T		A

Mechanické a elektronické šifrovacie stroje

- 1881 – Fleisner von Wostrowitz – mechanická pomôcka
- Vo štvorci $n \times n$ políčok sa vystrihne $n \times n/4$ políčok tak, aby pri postupnom otáčaní o 90 stupňov otvory ukazovali vždy na iné políčka.
- Políčka sa postupne zaplňajú. Šifrovaný text sa vypisuje po riadkoch.
- Jules Verne – Nový gróf Monte Christo,
- Nemecká armáda v I. sv. vojne – poľná šifra

Sifrovanie ta bavi



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

B			A
	V		
I			

Mechanické a elektronické šifrovacie stroje

- 1881 – Fleisner von Wostrowitz – mechanická pomôcka
- Vo štvorci $n \times n$ políčok sa vystrihne $n \times n/4$ políčok tak, aby pri postupnom otáčaní o 90 stupňov otvory ukazovali vždy na iné políčka.
- Políčka sa postupne zaplňajú. Šifrovaný text sa vypisuje po riadkoch.
- Jules Verne – Nový gróf Monte Christo,
- Nemecká armáda v I. sv. vojne – poľná šifra

Sifrovanie ta bavi



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

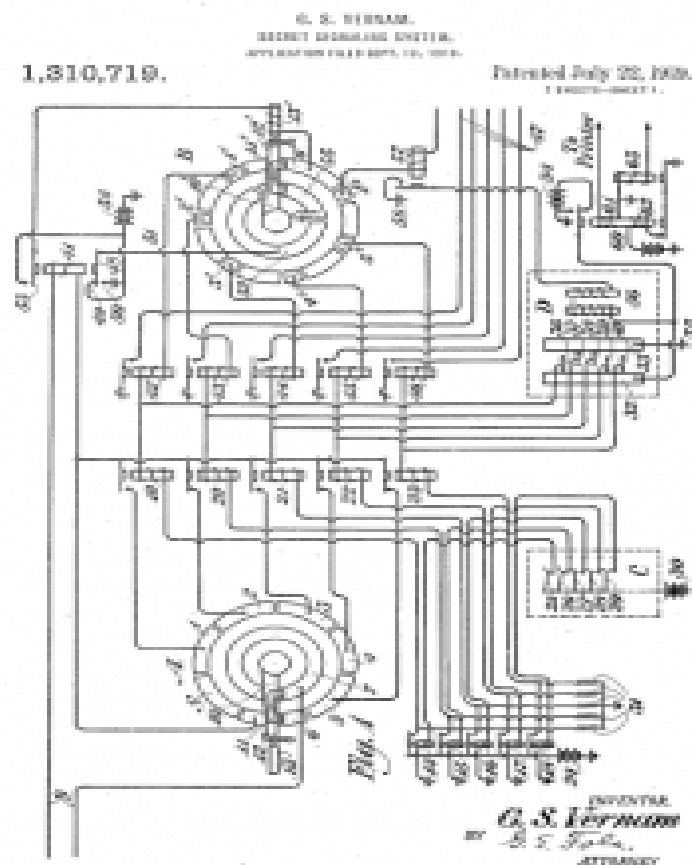
S	I	I	O
B	F	V	A
A	V	E	N
V	T	R	A

Mechanické a elektronické šifrovacie stroje

- 1917 - Gilbert S. Vernam – AT&T – polyalfabetický šifrovací stroj schopný používať náhodný neopakujúci sa kód. Do stroja sa vkladá dierna páska s otvoreným textom spolu s diernou páskou na ktorej bol náhodne vygenerovaný kľúč. Šifrogram vznikol sčítaním príslušných bitov obidvoch pásek modulo 2.
- Systém ostáva bezpečným, ak náhodný kľúč je rovnako dlhý ako šifrovaná správa a používa sa len raz (One Time Pad)



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED



Mechanické a elektronické šifrovacie stroje

- 1919 – Hugo Alexander Koch – patent šifrovacieho stroja založeného na rotoroch. Predal Arthurovi Scherbiusovi, ktorý ho vylepšil a nazval ENIGMA. Predstavená na medzinárodnom poštovom kongrese v Berne v roku 1923. Enigma nemala komerčný úspech. Používala sa v 2. sv. vojne nacistickým Nemeckom. Spôsob šifrovania rozlúštil Marian Rejewski, Alan Turing, Gordon Welchman



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED



Moderná vs. Klasická kryptografia

Klasická kryptografia	Moderná kryptografia
Používa tradičné znaky: čísla, písmená	Používa sekvencie binárnych znaky
Bezpečnosť na základe utajenia – security through obscurity	Používa známe matematické algoritmy pre kódovanie informácií. Bezpečnosť je daná utajením kľúča a matematickou zložitou algoritmov.
Komunikácia prebieha pomocou kryptografického systému, ktorý musia komunikujúce strany vlastniť.	Komunikácia môže prebehnúť medzi stranami, ktoré vlastnia len kľúče.

Kryptológia

Kryptografia

- návrh bezpečnostných schém na zabezpečenie doveryhodnosti, integrity a autenticity dát. (dostupnosť?)
- Veda o tajnom písme

Kryptoanalýza

- analýza kryptografických systémov, vstupov a výstupov, s cieľom odhaliť utajené premenné a/alebo citlivé dáta vrátane čistého textu.
- Veda o prelamovaní šifier

Steganografia

- utajenie existencie správy



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED



Kryptológia nie je len o matematike ale aj technologickej implementácii kryptografických algoritmov a architektúr, ako aj o implementácii kryptoanalytických metód, techník a nástrojov.

Alica, Bob, Eva a ostatní

Kryptografia:

Zabezpečuje súkromie,
dôvernosť a autentifikáciu

Nezabezpečuje integritu,
nechráni pred ukradnutím
správy

Symetrické šifrovanie – rovnaký
kľúč na šifrovanie aj
dešifrovanie

Asymetrické šifrovanie –
súkromný a verejný kľúč



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

Alice, Bob and Eve





Symetrická šifra

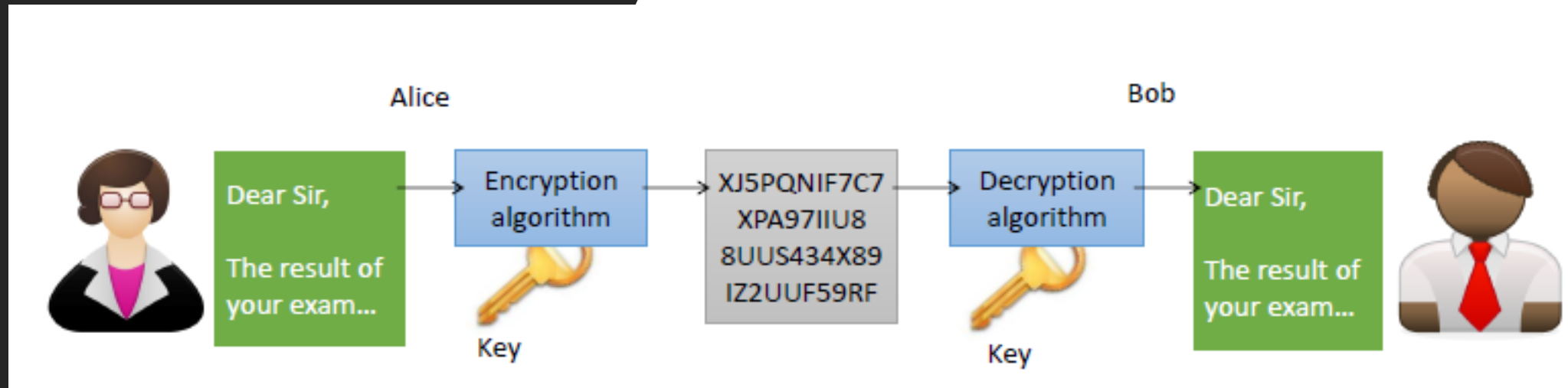
- Šifrovanie:

$E: P \times K \longrightarrow C$

- Dešifrovanie:

$D: C \times K \longrightarrow P$

$$\forall k \in K \forall p \in P: D_k(E_k(p)) = p$$



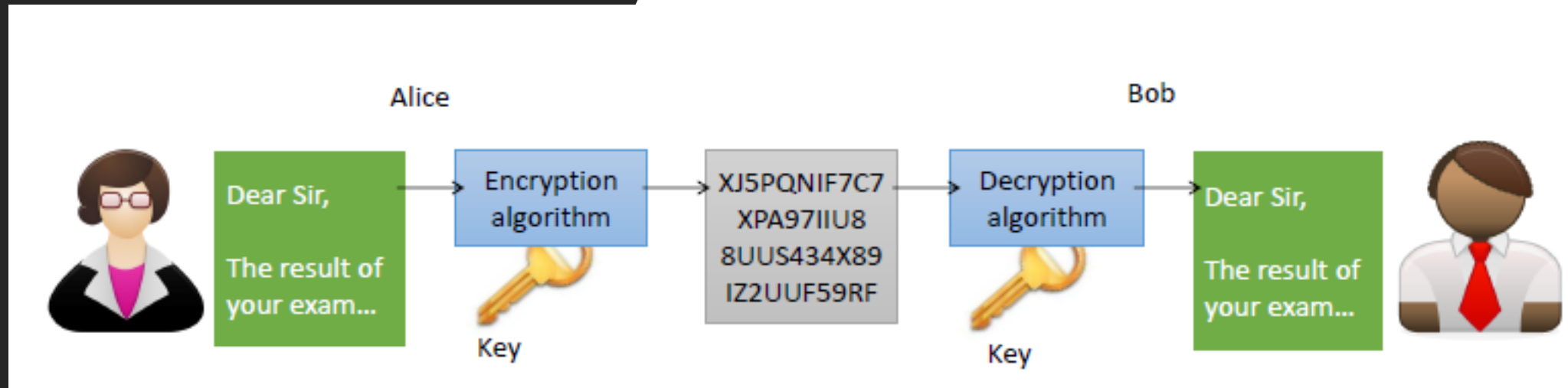
Bezpečnosť symetrickej šifry

- nedá sa získať zmysluplná informácia o otvorenom texte pre známy šifrovaný text
- nedá sa vypočítať funkcia nad otvoreným textom pre známy šifrovaný text



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

$$\forall k \in K \forall p \in P: D_k(E_k(p)) = p$$



AES, DES, 3DES

AES

- AES 128 – 10 cyklov
- AES 192 – 12 cyklov
- AES 256 – 14 cyklov

Pripočítanie podkľúča, substitúcia bytov, posun riadkov, miešanie stĺpcov

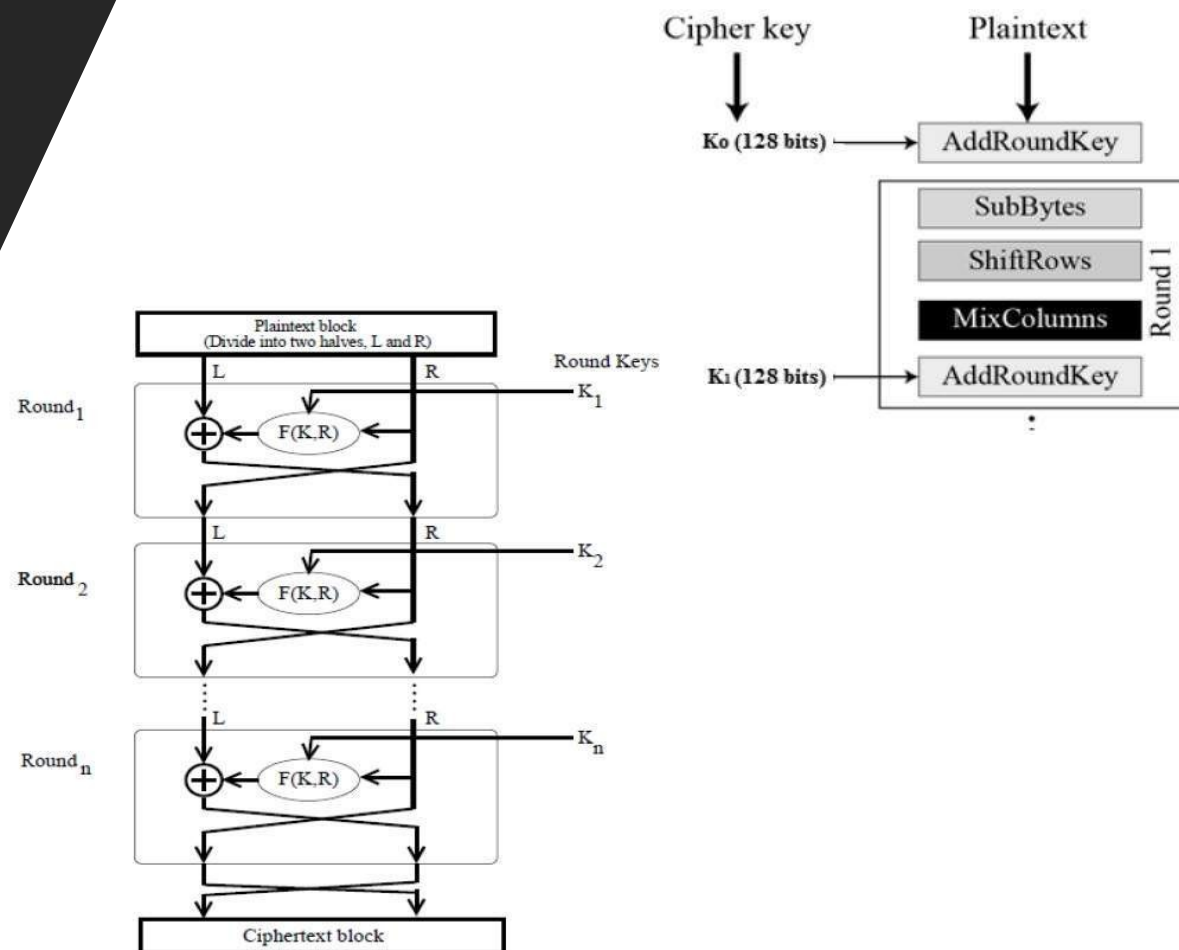
DES

Lavínový efekt – malá zmena v otvorenom texte sa prejaví veľkou zmenou v šifrovanom texte

Úplnosť – každý bit šifrovaného textu závisí na ďalších bitoch otvoreného textu

3DES

- $E(P) = E'_{K3}(D'_{K2}(E'_{K1}(P))) = C$
- $D(C) = D'_{K1}(E'_{K2}(D'_{K3}(C))) = P$



Asymetrická šifra

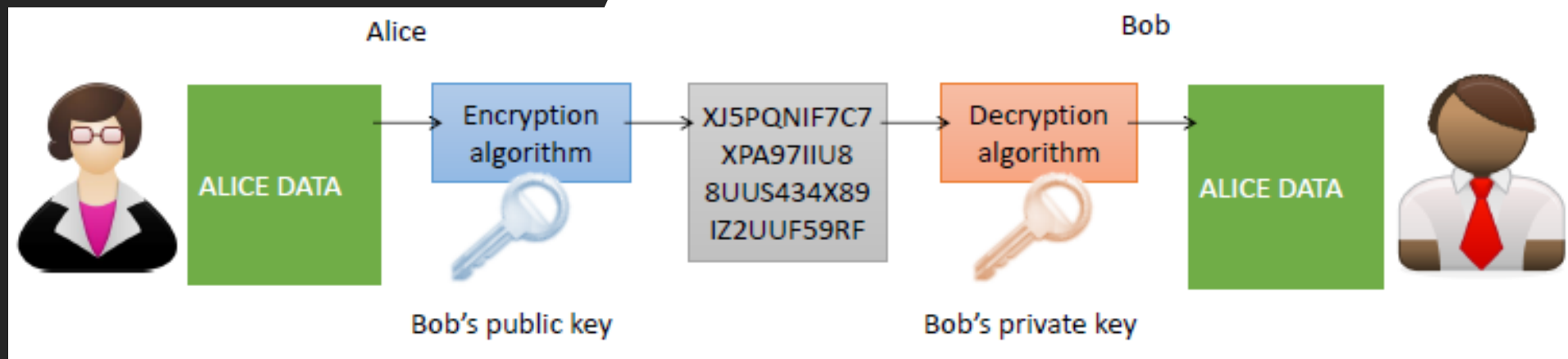
Dvojica rôznych kľúčov

verejný – šifrovanie

súkromný – dešifrovanie



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED



Asymetrická šifra

Príklady: RSA, ElGamal

Ron Rivest, Adi Shamir, and Leonard Adleman 1977

RSA schéma:

- Súkromný kľúč (d, n)
- Verejný kľúč (e, n)
- $n = p * q$
- e je nesúdeliteľné s $(p-1)(q-1)$
- $e * d \equiv 1 \pmod{(p-1)(q-1)}$
- $E(x) = x^e \pmod{n}$
- $D(c) = c^d \pmod{n}$



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

$$p = 3, q = 11$$

$$n = 3 * 11 = 33$$

$$e = 3 \text{ nesúdeliteľné s } 2 \times 10 = 20$$

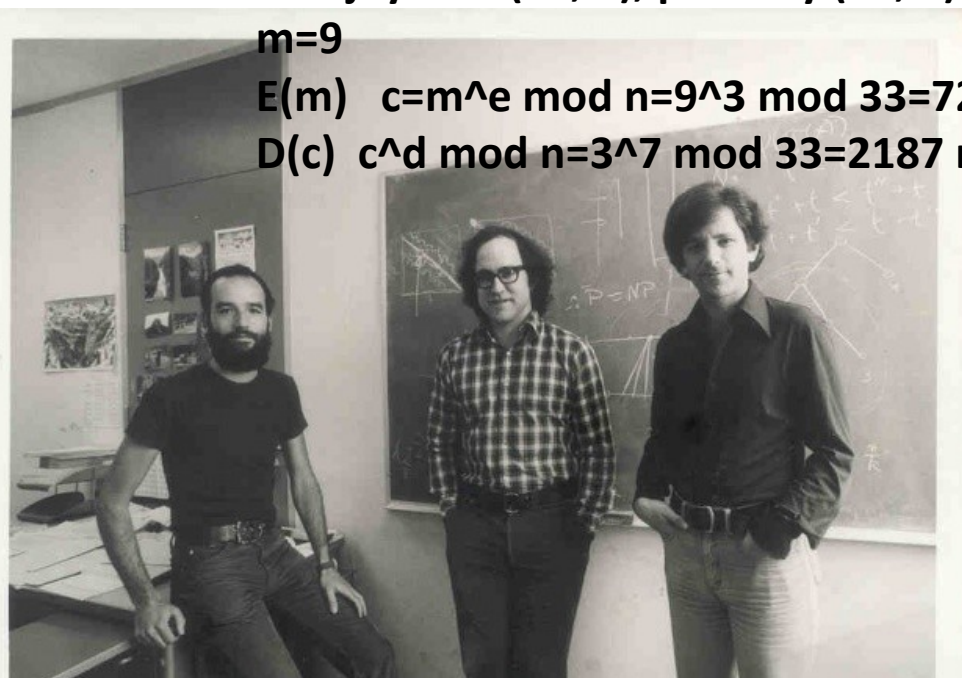
$$d = 7, \text{ lebo } 3 * d \pmod{20} = 1$$

Verejný kľúč $(33, 3)$, privátny $(33, 7)$

$$m = 9$$

$$E(m) \quad c = m^e \pmod{n} = 9^3 \pmod{33} = 729 \pmod{33} = 3$$

$$D(c) \quad c^d \pmod{n} = 3^7 \pmod{33} = 2187 \pmod{33} = 9$$



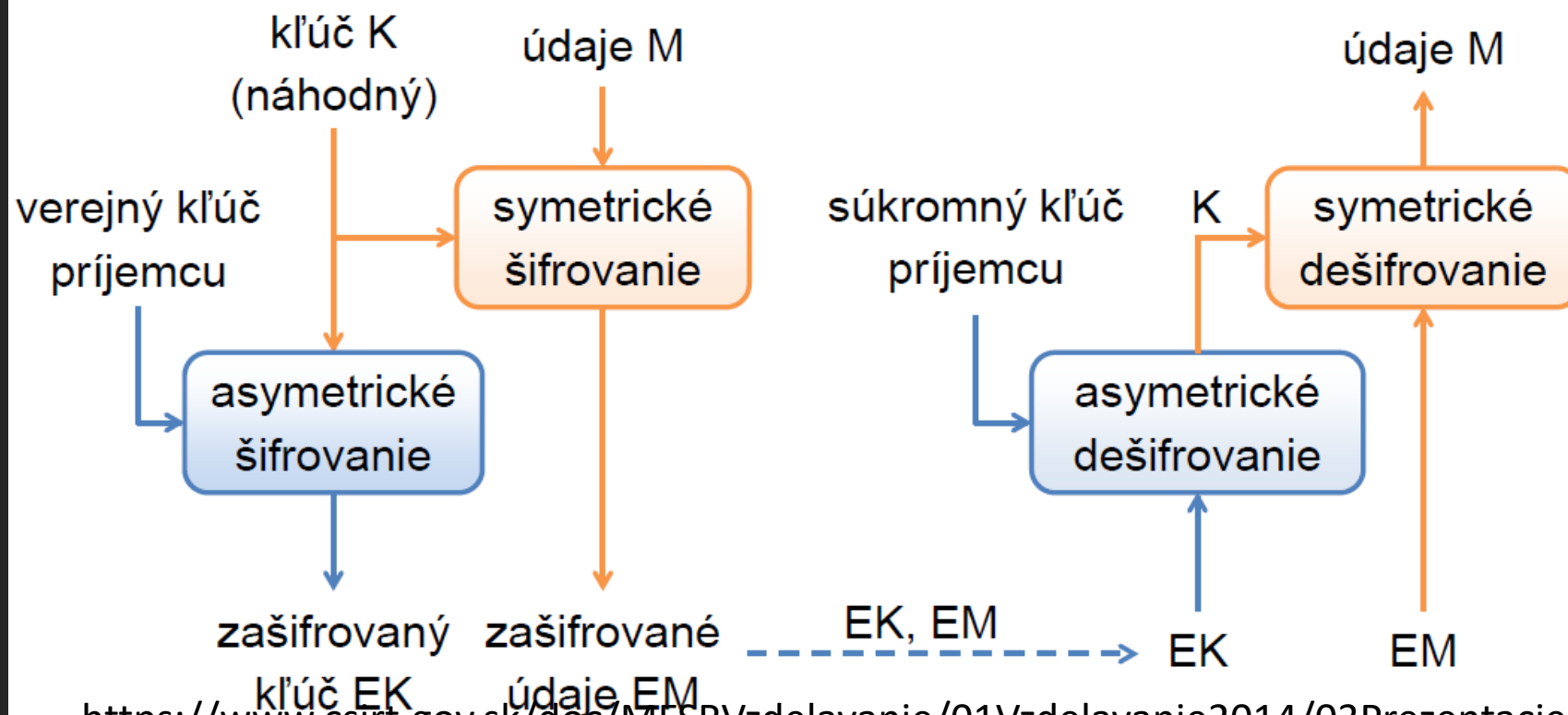
Hybridné šifrovanie

Symetrické šifrovanie na dlhé texty

Asymetrické šifrovanie na kľúč



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED



Ďakujem za
pozornosť

Ivana.Budinska@savba.sk



ÚSTAV INFORMATIKY
SLOVENSKÁ AKADEMIA VIED

