Vybrané kapitoly z kryptografie

(Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti“ – modul č. 2)

Meno a priezvisko

XX.XX.XXXX

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

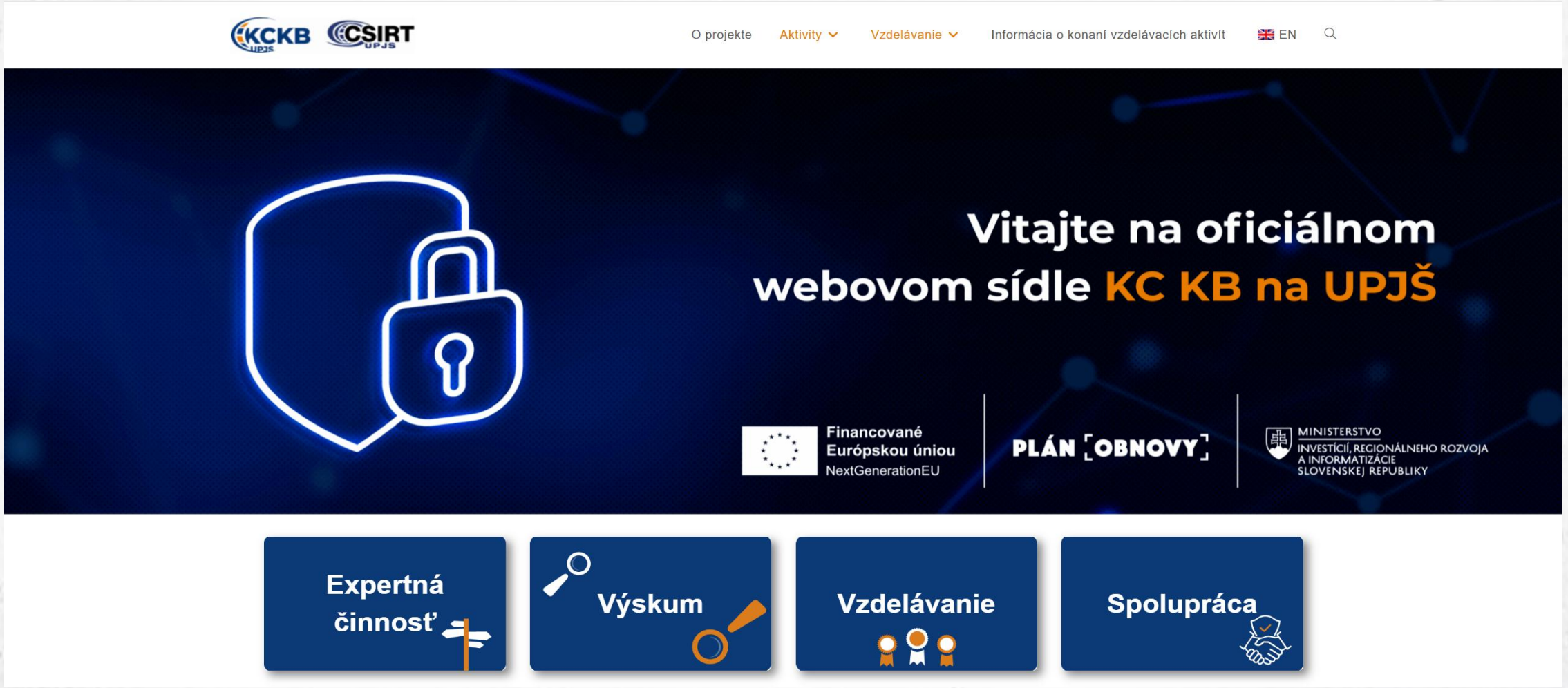
Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KC KB UPJŠ

https://**cyberawareness.sk/**



Vzdelávacia aktivita (I.)

- Časový harmonogram
  - 08:30 – 10:00 – 1. blok
  - 10:00 – 11:30 – 2. blok
  - 11:30 – 12:30 – obedňajšia prestávka
  - 12:30 – 14:00 – 3. blok
  - 14:00 – 15:30 – 4. blok

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Vzdelávacia aktivita (II.)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	**Úvod do KIB a riadenie KIB**	8	Online / Prezenčne
Modul č. 2	**Vybrané kapitoly z kryptografie**	8	Prezenčne
Modul č. 3	**Vybrané kapitoly zo sieťovej bezpečnosti**	16	Prezenčne
Modul č. 4	**Reaktívne a proaktívne činnosti**	8	Prezenčne
Modul č. 5	**Reaktívne činnosti – komunikácia**	6	Prezenčne
Modul č. 6	**Vybrané kapitoly z práva informačných a komunikačných technológií I.**	8	Online / Prezenčne
Modul č. 7	**Vybrané kapitoly z práva informačných a komunikačných technológií II.**	8	Online / Prezenčne

Kryptológia

- grécky kryptós (κρυπτός) = ukrytý
- -logia (-λογία) = štúdium
- -graphein (-γράφειν) = písanie
- **kryptografia** – štúdium algoritmov (protokolov) pre bezpečnú komunikáciu
- **kryptoanalýza** – vyhľadávanie bezpečnostných slabín v algoritmoch (protokoloch) a možností ich využitia pri získavaní utajených informácií
- **steganografia** - ukrývanie správy v texte/obrázku

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Úvod do kryptografie a klasické šifry

Využitie kryptografie

- utajenie prenosu informácie (dôvernosť komunikácie)
- zabezpečenie proti zmenám pri prenose (integrita správ)
- zabezpečenie proti výmene a podhodeniu nepravých správ (pôvodnosť správ)
- zabezpečenie proti maskovaniu sa odosielateľa za iného (nepopierateľnosť pôvodcu správy)
- obmedzenie zahltenia informačného zdroja (dostupnosť správ)
- iné nástroje na dosiahnutie komunikačnej bezpečnosti ...

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kódovanie

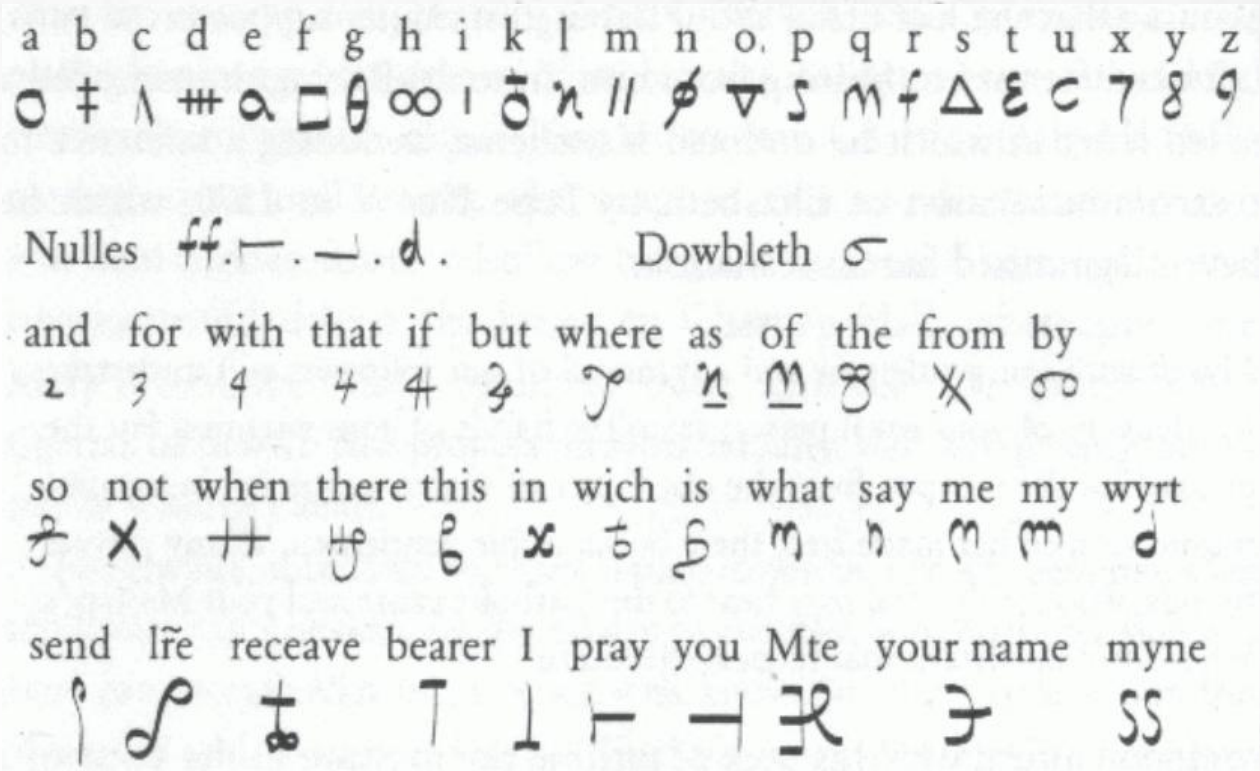
- kto pozná kód (algoritmus kódovania), ten vie správu prečítať

- KRYPTOGRAFIA NA UPJS JE SUPER!
- 4b525950544f47524146494120e412055504a53204a452053550455221 - ASCII kódovanie
- UPJS的密碼學是偉大的！
- التشفيرعلى أوبس هو عظيم!
- クリプトグラフィア・ナー・アップジズ・
- ジー・スーパー

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kódové knihy

Mária Stuartová – správy šifrované kódom (nomenklátorom)



https://www.simonsingh.net/The_Black_Chamber/z_cipherimages/maryqueenimage.gif

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Steganografia

MKJEDKKJFMERMFJEDYJEPSEPJFKSTTJFKSTOFWSAS
GMLKOPRJEDTSAMLKPOFYTDHFIJEQWIAMLDKENM
LPQOADRTYLUDLPORPAQWLMJMLDKTSLKDPTJLKD
PTELKDTSSDPEOTULDKTAPDRLGHETRSALRSELTM

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Steganografia

- MKJEDKKJFMERMFJEDYJEPSEPJFKSTTJFKSTOFWSAS
  GMLKOPRJEDTSAMLKPOFYTDHFIJEQWIAMLDKENM
  LPQOADRTYLUDLPORPAQWLMJMLDKTSLKDPTJLKD
  PTELKDTSSDPEOTULDKTAPDRLGHETRSALRSELTM

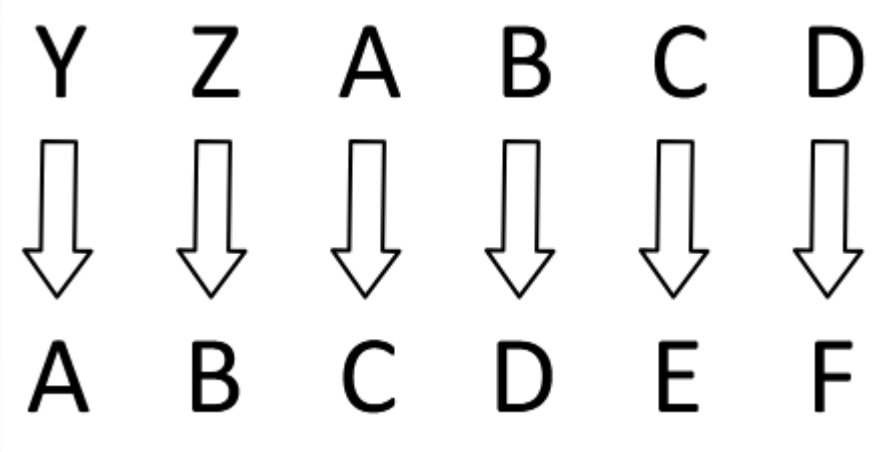
- MKJED K KJFME R MFJED Y JEPSE P JFKST T JFKST O
  FWSAS G MLKOP R JEDTS A MLKPO F YTDHF I
  JEQWI A MLDKE N MLPQO A DRTYL U DLPOR P
  AQWLM J MLDKT S LKDPT J LKDPT E LKDTS S DPEOT
  U LDKTA P DRLGH E TRSAL R SELTM

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Posuvná šifra

abecedný posun o k znakov abecedy

- k je tajomstvo medzi odosielateľom a prijímateľom správy
- 25 možných posunov v anglickej abecede



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kryptoanalýza

H	O	V	M	Q	L	D	O	X	C	F	X		K	X		R	M	G	P		G	B		P	R	M	B	O	!

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kryptoanalýza

H	O	V	M	Q	L	D	O	X	C	F	X		K	X		R	M	G	P		G	B		P	R	M	B	O	!

								A			A			A															!

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kryptoanalýza

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

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Afinný kryptosystém

Písmená nahradíme číslami {0, 1, ..., 25}

- kľúč K = { (a, b) | $a \in$ {1,3,5,7,9,11,15,17,19,21,23,25}, $b \in$ {0, 1, ..., 25} }
- šifrovanie e(x) = (ax + b) mod 26
- dešifrovanie $d(y) = a' \, y - b$ mod 26

  kde a' je inverzný prvok k a teda $a' \, . \, a$ mod 26 = 1

  to existuje práve vtedy, keď nsd (a, 26) = 1
- 26 x 26 x 12 = 312 možností

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Monoalfabetická substitúcia

- tajomstvom je zvolená permutácia abecedy
- permutácií je 26! = 403 291 461 126 605 635 584 000 000

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

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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Monoalfabetická substitúcia

Ako si zapamätať kľúč ?

VELMIUTAJNYKCBDFGHOPQRSWXZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

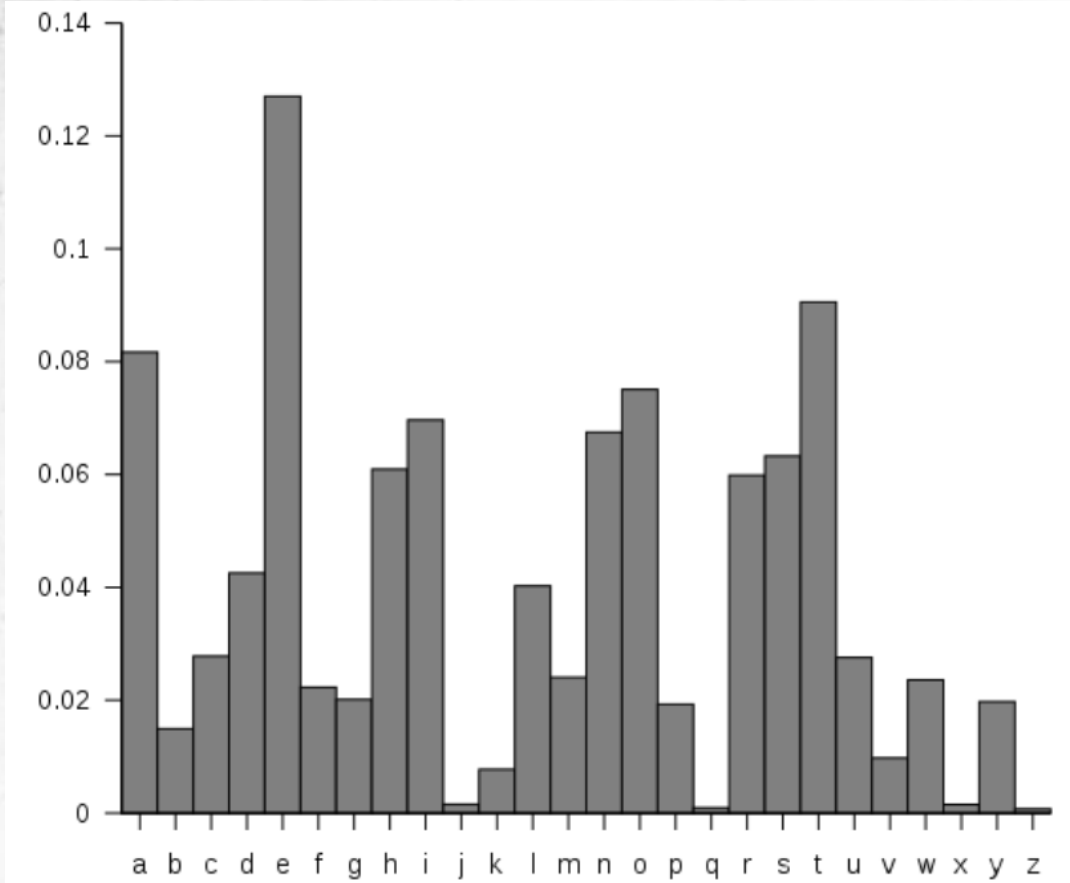
Monoalfabetická substitúcia

Možnosti kryptoanalýzy monoalfabetickej substitúcie

- jazyk otvoreného textu
- medzery, predložky, spojky ...
- opakované sekvencie, známe časti textu (začiatok, koniec)
- frekvencia výskytu znakov - frekvenčná analýza

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Monoalfabetická substitúcia



https://upload.wikimedia.org/wikipedia/commons/d/d5/English_letter_frequency_%28alphabetic%29.svg

- písmená podľa frekvencie
- krátke slová (THE, IS)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kryptoanalýza

- COA (ciphertext only attack)
  poznáme len šifrovaný text, algoritmus šifrovania a charakteristiku otvoreného textu
- KPA (known-plaintext attack)
  poznáme aspoň jednu dvojicu otvoreného a šifrovaného textu
- CPA (chosen-plaintext attack)
  môžeme si nechať niečo zašifrovať
- CCA (chosen-ciphertext attack)
  môžeme si nechať niečo dešifrovať
- adaptívne varianty CPA a CCA

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kryptoanalýza

- postranné kanály (side channels attack)
- chyby v implementácii
- malware, spyware, ransomware …
- sociálne inžinierstvo, phishing …
- korupčná kryptoanalýza
- pendreková (rubber-hose) kryptoanalýza

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Obrana pred frekvenčnou analýzou

- homofónne šifry – monoalfabetické substitúcie, kde sa priradí frekventovaným znakom otvoreného textu náhodne jeden z viacerých znakov šifrovaného textu (napr. e(E) ∈ {X,Y}; e(I) = e(J) = Z; a pri dešifrovaní sa I a J rozlíši podľa kontextu)

- bigramové šifry – substitúcia po dvojiciach znakov (pri veľmi dlhom texte by mohla kryptoanalýze pomôcť frekvenčná analýza bigramov)

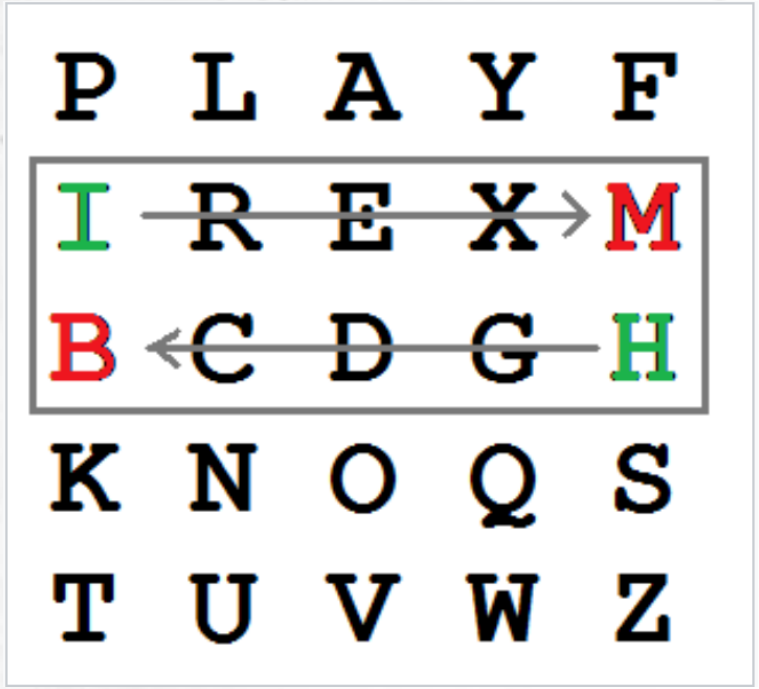
- polygramové a polyalfabetické šifry

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Šifra Playfair

- bigramová šifra (Ch. Wheatstone 1854)

https://en.wikipedia.org/wiki/Playfair_cipher



th 1.52	en 0.55	ng 0.18
he 1.28	ed 0.53	of 0.16
in 0.94	to 0.52	al 0.09
er 0.94	it 0.50	de 0.09
an 0.82	ou 0.50	se 0.08
re 0.68	ea 0.47	le 0.08
nd 0.63	hi 0.46	sa 0.06
at 0.59	is 0.46	si 0.05
on 0.57	or 0.43	ar 0.04
nt 0.56	ti 0.34	ve 0.04
ha 0.56	as 0.33	ra 0.04
es 0.56	te 0.27	ld 0.02
st 0.55	et 0.19	ur 0.02

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Hillova šifra

Lester Hill (1929) polygramová šifra (m-prvkové vektory kódov znakov, násobenie maticami)

pre matice 2 x 2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (\mathrm{ad} - \mathrm{bc})^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

príklad

$k = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ HELP $\begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ P \end{pmatrix}$ $p = \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 11 \\ 15 \end{pmatrix}$

$e_k(p) = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 8 \end{pmatrix} \ (mod\ 26)$, $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 19 \end{pmatrix} \ (mod\ 26)$

$c = \begin{pmatrix} 7 \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 19 \end{pmatrix}$ $\begin{pmatrix} H \\ I \end{pmatrix}, \begin{pmatrix} A \\ T \end{pmatrix}$ HIAT

$d_k(e_k(p)) = 9^{-1} \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 4 \end{pmatrix} \ (mod\ 26) \quad \ldots \begin{pmatrix} H \\ E \end{pmatrix}$

$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 15 \end{pmatrix} \ (mod\ 26) \ldots \begin{pmatrix} L \\ P \end{pmatrix}$

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Polyalfabetická šifra

využívajú viacero abecied

šifrovacia a dešifrovacia funkcia závisí aj od pozície znaku v texte

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

PT	K	R	Y	P	T	O	G	R	A	F	I	A		N	A		U	P	J	S		J	E		S	U	P	E	R	!
	B	O	E	M	W	J	I	O	G	Y	Z	G		C	G		H	M	P	T		P	N		T	H	M	N	O	
	M	A	P	V	S	W	J	A	H	R	L	H		K	H		C	V	I	B		I	E		B	C	V	E	A	
CT	B	A	E	V	W	W	I	A	G	R	Z	H		C	H		H	V	P	B		P	E		T	C	M	E	O	

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Vigenerova šifra

- Giovan Battista Bellaso (1553)
- tabula recta (Trithemius 1508)
- neskôr omylom pripísaná Blaise de Vigenèrovi

posuvná šifra s posunom, závislým od pozície znaku v texte

posun určuje kľúčové slovo (expandované na dĺžku otvoreného textu)

	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

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Vigenerova šifra - kryptoanalýza

1. nájdeme dĺžku kľúča r
   Kasiského metóda (1863, tiež Babbage 1846) vzdialenosti medzi opakujúcimi sa reťazcami znakov v šifrovom texte sú s veľkou pravdepodobnosťou násobkami dĺžky kľúča
2. nájdeme kľúč
   stačí analyzovať postupnosti
   $(y_1\ y_{r+1}\ y_{2r+1}\ y_{3r+1}\ ..)$, $(y_2\ y_{r+2}\ y_{2r+2}\ y_{3r+2}\ ..)$, …, $(y_r\ y_{2r}\ y_{3r}\ ..)$
   šifrového textu pomocou frekvenčnej analýzy/vektormi pravdepodobností
   postupne nájdeme posuny, z ktorých rekonštruujeme kľúč

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kerckhoffs (1883) - La cryptographie militaire

- kryptografický systém je bezpečný, ak útočník nie je schopný dešifrovať text ani vtedy, keď dokonale pozná postup šifrovania

Dôvernosť komunikácie je zabezpečená len znalosťou kľúča

- kľúč je zapamätateľný a ľahko modifikovateľný
- šifrovaný text je možné prenášať telegraficky
- šifrovacie/dešifrovacie zariadenia musia byť prenosné a ľahko používateľné a nemali by vyžadovať od používateľa dodržiavanie dlhého zoznamu pravidiel
- systém by mal byť prakticky nedešifrovateľný

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

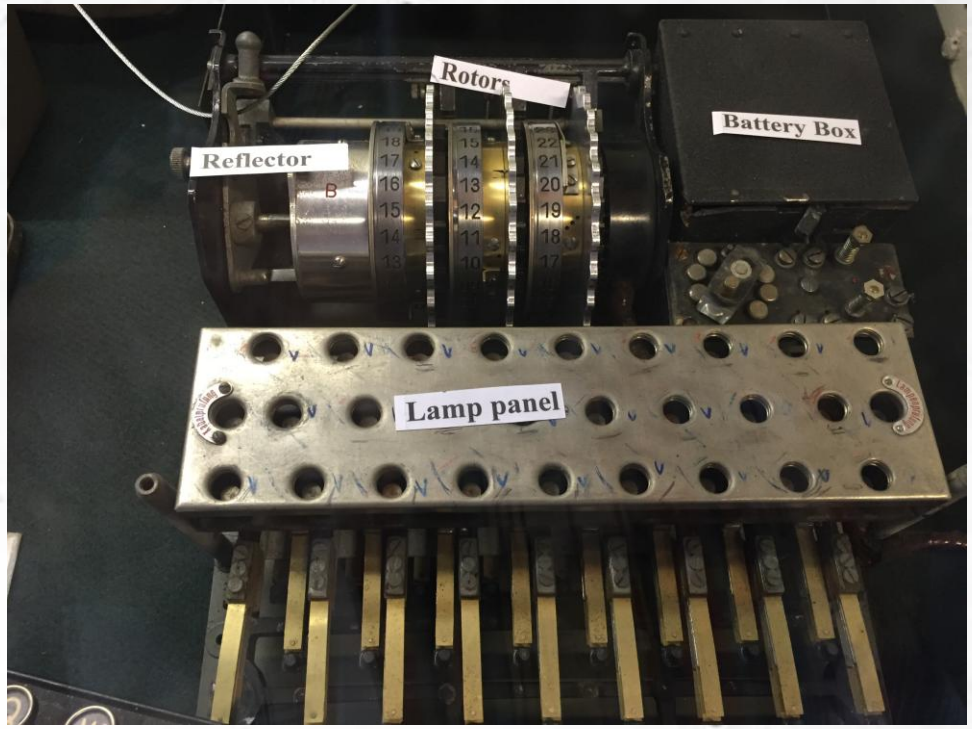
Enigma

- elektromechanický rotorový šifrátor
- Arthur Scherbius (1918)

komerčne dostupný (cca 100000 kusov)

- vojenské modely s rôznymi vylepšeniami
- šifra prelomená tesne pred začiatkom vojny

(30 rokov v utajení)



https://upload.wikimedia.org/wikipedia/commons/b/ba/Enigma_insides.agr.jpg

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Transpozičné šifry

Šifrový text vznikne permutáciou (niektorých) znakov otvoreného textu (ak je text dlhý, možno ho rozdeliť na bloky podľa veľkosti permutácie)

- zápis otvoreného textu odzadu
- zápis textu do riadkov pevnej dĺžky a šifrovanie čítaním po stĺpcoch (scytale)
- stĺpcová transpozícia – pred čítaním stĺpce zamiešame
- permutačné mriežky (jednoduché zapamätanie permutácie – mechanické šifrovanie a dešifrovanie)

expanzná permutácia - zobrazenie znakov otvoreného textu na viacero miest šifrového textu (eliminácia použitia frekvenčnej analýzy a hľadania anagramov)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Šifra ADFGX

používaná v 1. svetovej vojne v nemeckej armáde

- kombinácia Polybiovho štvorca so stĺpcovou transpozíciou
- znaky šifrového textu – A D F G X – odlišný Morseho kódu (redukcia chýb)
- kľúč (napr. „VELMINAHODNE ABEZPECNEHESLO“) zapíšeme do Polybiovho štvorca (ako v Playfair šifre)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Šifra ADFGX

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

znaky otvoreného textu šifrujeme dvojicou indexu riadku a indexu stĺpca

K R Y P T O G R A F I A

GF GX XX FF XA DG GD GX DD GA AX DD

S	U	P	E	R
G	F	G	X	X
X	F	F	X	A
D	G	G	D	G
X	D	D	G	A
A	X	D	D	

E	P	R	S	U
X	G	X	G	F
X	F	A	X	F
D	G	G	D	G
G	D	A	X	D
D	D	**X**	A	X

a pokračujeme **stĺpcovou transpozíciou** s kľúčom SUPER

šifrový text (po stĺpcoch):

XXDGD GFGXD XAGAX GXDXA FFGDX

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou
NextGenerationEU

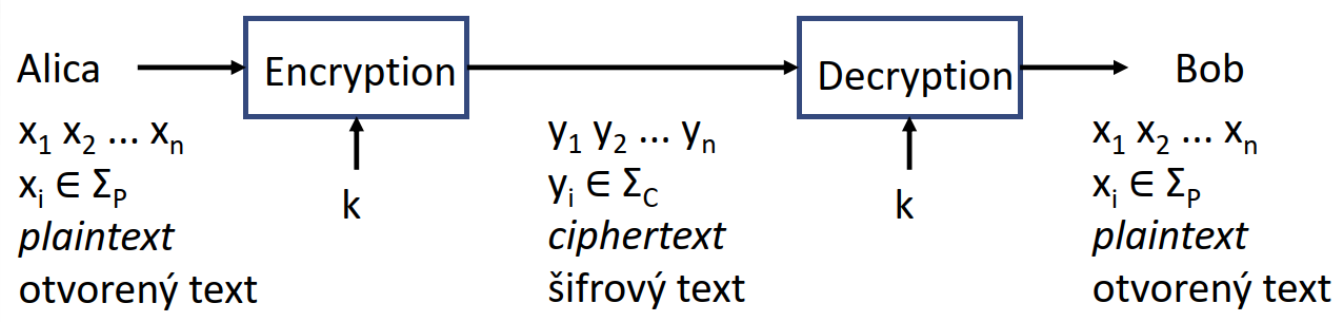
PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Symetrické algoritmy

Symetrické šifrovacie systémy

Na šifrovanie aj dešifrovanie sa používa ten istý kľúč



- **blokové**
  správa sa rozdelí na bloky a šifruje sa naraz celý blok blokovou šifrou (teda pevnej veľkosti)
- **prúdové**
  prúd bitov sa modulárne pripočíta (xor) k správe

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

bezpečnosť

dokázateľná bezpečnosť (provable security)

- problém nájdenia kľúča je možné previesť na problém s dostatočnou zložitosťou, ktorý zatiaľ nevieme vyriešiť

výpočtová bezpečnosť (computational security)

- známe postupy na hľadanie kľúča nie sú v rozumnom čase známymi prostriedkami (konštrukčnými, energetickými, finančnými) uskutočniteľné

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

bezpodmienečná bezpečnosť (unconditional security)

- perfect secrecy
- pravdepodobnosť uhádnutia otvoreného textu ak poznáme šifrovaný text je rovnaká, ako keby sme ho nepoznali
- celý kľúč nemôže byť prelomený ani nekonečne veľkou výpočtovou silou
- *Shannon*: šifrovanie je bezpodmienečne bezpečné práve vtedy, ak každý kľúč je použitý s rovnakou pravdepodobnosťou a dĺžka kľúča aj textu je rovnaká
- *Vernam* 1917 (Vigenerova šifra)
- xor s náhodným a utajeným kľúčom použitý práve raz

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prúdové šifrovacie systémy

prúd - stream (pseudo)náhodne generovaný

- utajený kľúč (počiatočné nastavenie generátora – seed)
- nesmie sa použiť viackrát
- problémy s integritou !

  negáciou bitov šifrového textu je možné cielene zmeniť bity v dešifrovanom texte

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prúdové šifrovacie systémy

TRNG (True random number generator)

hw riešenie (tepelný šum, kvantové javy, udalosti v PC)

na dešifrovanie preniesť ďalším bezpečným kanálom !

PRNG – generátory pseudonáhodných čísel

generovanie závisí (deterministicky) len od počiatočného nastavenia - kľúča (seed)

LFSR – lineárne posuvné registre so spätnou väzbou $s_n = (s_{n-1}a_{m-1} + \ldots + s_{n-m+1}a_1 + s_{n-m}a_0) \bmod 2$

CSPRNG – kryptograficky bezpečné pseudonáhodných čísel

výstup nie je možné predikovať (dokázateľne)
Blum-Blum-Shub generátor

$$b_{i+1} = b_i^2 \; mod \; pq \qquad p \equiv q \equiv 3 \; (mod \; 4)$$
$$s_{i+1} = b_{i+1} \; mod \; 2$$

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prúdové šifrovacie systémy

TRNG (True random number generator)

hw riešenie (tepelný šum, kvantové javy, udalosti v PC)

na dešifrovanie preniesť ďalším bezpečným kanálom !

PRNG – generátory pseudonáhodných čísel

generovanie závisí (deterministicky) len od počiatočného nastavenia - kľúča (seed), perióda

LFSR – lineárne posuvné registre so spätnou väzbou $s_n = (s_{n-1}a_{m-1} + \ldots + s_{n-m+1}a_1 + s_{n-m}a_0) \bmod 2$

CSPRNG – kryptograficky bezpečné pseudonáhodných čísel

výstup nie je možné predikovať (dokázateľne)
Blum-Blum-Shub generátor

$b_{i+1} = b_i^2 \ mod \ pq \qquad p \equiv q \equiv 3 \ (mod \ 4)$

$s_{i+1} = b_{i+1} \ mod \ 2$

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prúdové šifrovacie systémy

- A5/1 (GSM)
- SNOW (3G)
- SNOW-V (5G)
- E0 (BlueTooth)
- RC4 (čipové karty/WEP, Rivest 1987)

EU CRYPT (2012) – HC-128, Rabbit, Salsa20, SOSEMANUK, Grain, MICKEY, Trivium

NIST (2019) – ASCON (IoT)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Symetrické šifrovacie systémy

- substitučné
- transpozičné

Shannon (1945) entropiu zvyšuje:

- konfúzia
  - zakrýva vzťah medzi kľúčoma šifrovým textom
  - zmena v kľúči spôsobí zmenu CT na viacerých miestach
  - zobrazenie je nelineárne
- difúzia
  - zakrývajúce vzťah medzi otvoreným a šifrovým textom
  - lavínový efekt

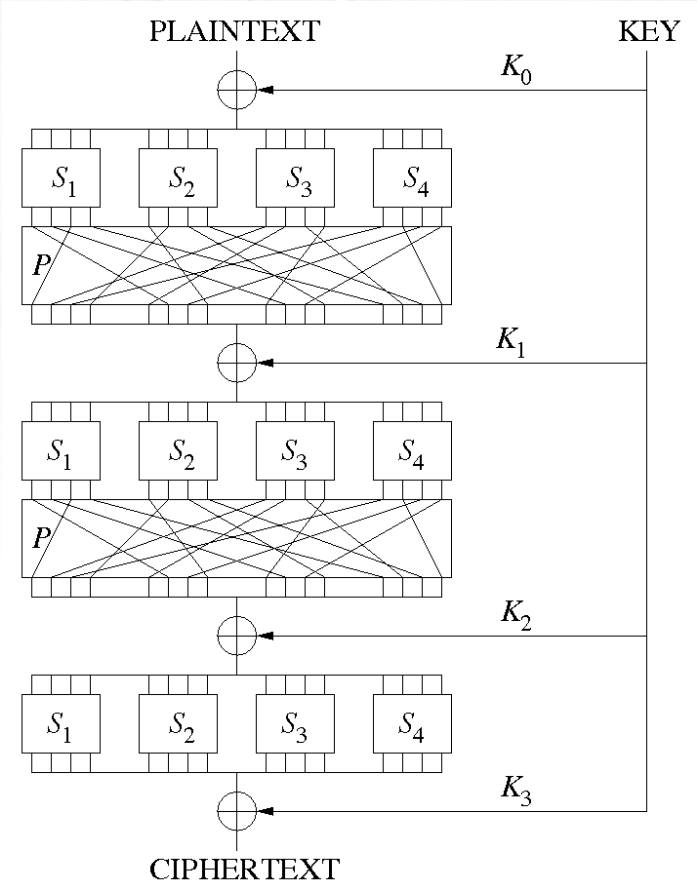
zloženie konfúzneho a difúzneho zobrazenia nie je komutatívne (záleží na poradí)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Substitučno – permutačné siete

substitučno-permutačné siete

- opakujú substitúciu (stále s iným kľúčom) a permutáciu vo viacerých kolách (round)
- účinnosť závisí od kvality:
  - substitučných blokov (S-boxov)
  - veľkosti permutácie (P-boxy)
- dešifrovanie – obrátený postup (s inverznými S-boxami)



https://upload.wikimedia.org/wikipedia/commons/c/cd/SubstitutionPermutationNetwork2.png

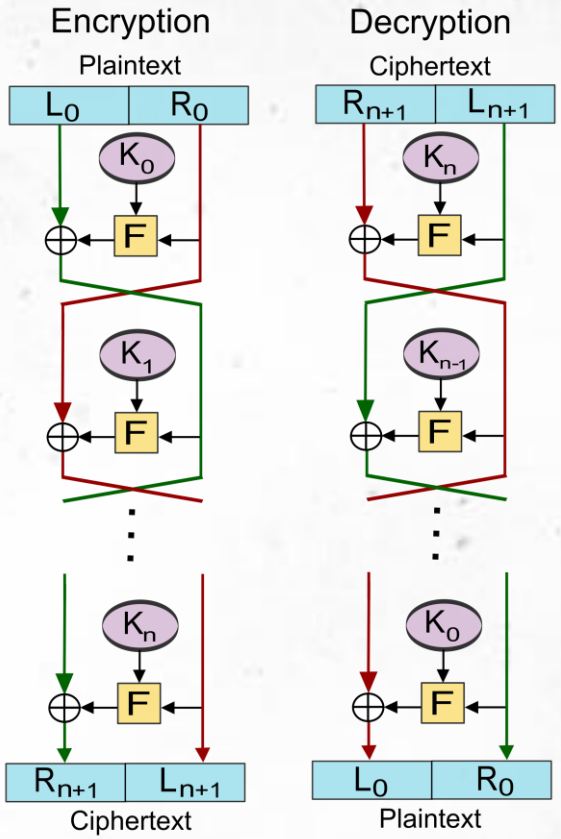
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Blokové symetrické šifry

Feistelova schéma (1973)

blok rozdelený na polovice, difúzia s opačnou polovicou bloku

- šifra Lucifer (IBM)
- DES (Digital Encryption Standard)
  - 64-bitový blok, 16 kôl
  - 4 slabé kľúče, 12 poloslabých
  - nehomomorfná šifra
  - 1977: 1 deň $20mil, 2017: rainbow table za 25s
- 3DES (Triple DES) $C = DES_{k_3}(DES_{k_2}^{-1}(DES_{k_1}(P)))$
- DES-X $C = k_3 \oplus DES_{k_1}(P \oplus k_2)$
- Blowfish



https://upload.wikimedia.org/wikipedia/commons/f/fa/Feistel_cipher_diagram_en.svg

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

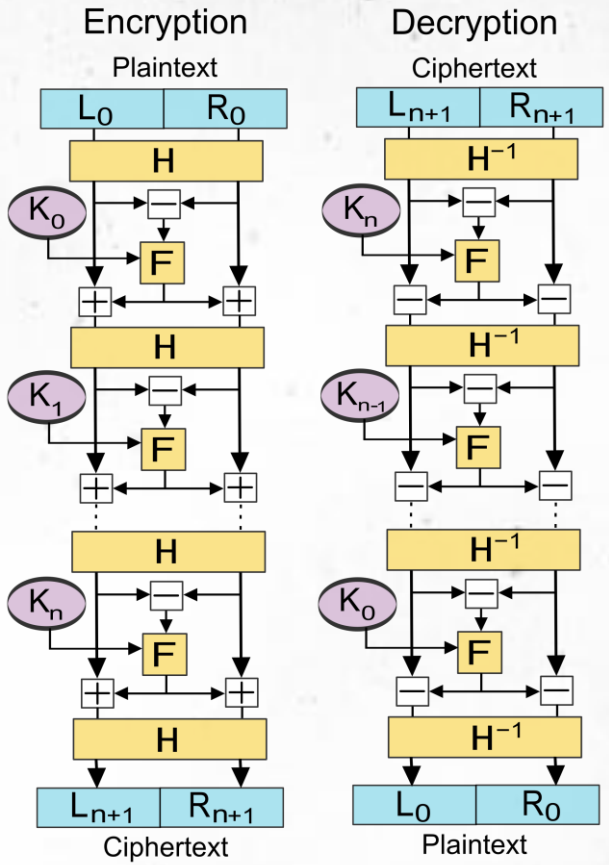
Blokové symetrické šifry

Lai-Massey schéma

Obehová funkcia sa však aplikuje na rozdiel medzi týmito dvoma časťami a výsledok sa potom pripočíta k obom polovičným blokom.

IDEA (1991 International Data Encryption Algorithm)

64-bitový blok, 128-bitový kľúč, 8 kôl



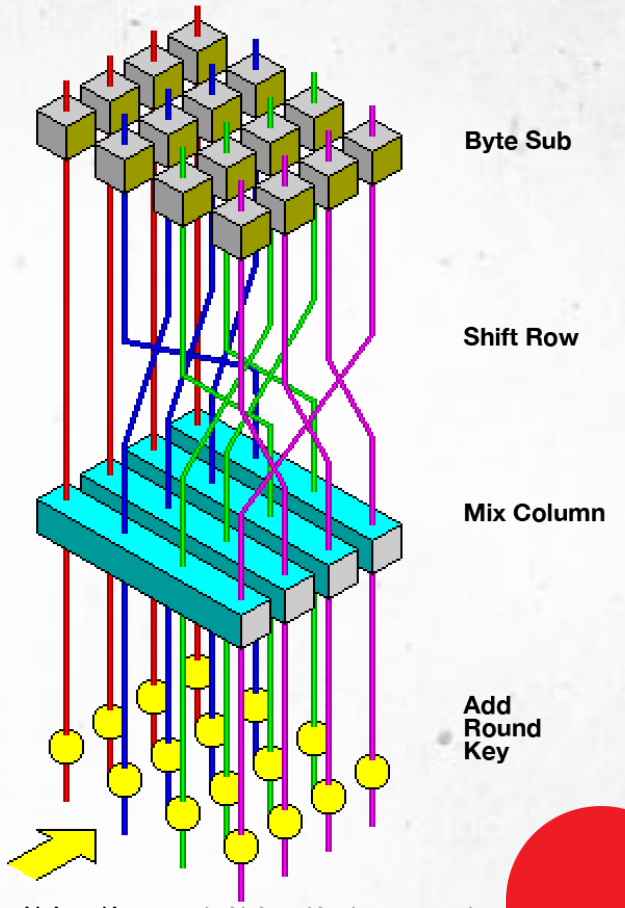
https://upload.wikimedia.org/wikipedia/commons/4/4f/Lai_Massey_scheme_diagram_en.svg

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Advanced Encryption Standard

NIST – 1997-2000 – konkurz na novú blokovú šifru

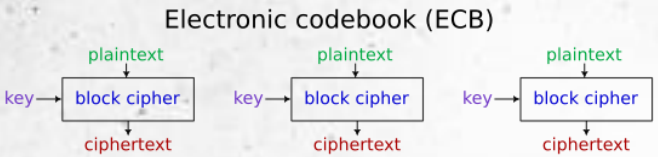
- 128 bitové bloky
- 128, 192, 256- bitové kľúče
- pre rôzne typy procesorov
- „lepší“ ako 3DES
- 1999 finalisti Pars, RC6, Rijndael, Serpent, Twofish
- 2001 za AES bol vybratý Rijndael (Rijmen, Daemen)

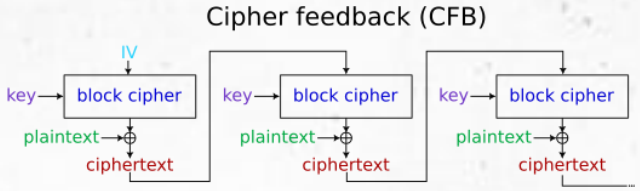


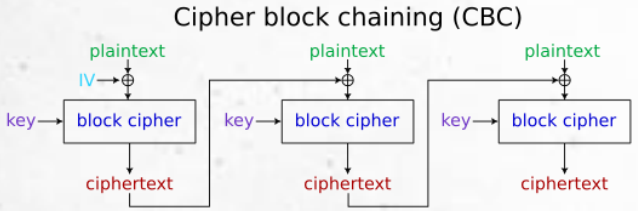
https://upload.wikimedia.org/wikipedia/commons/5/50/AES_%28Rijndael%29_Round_Function.png

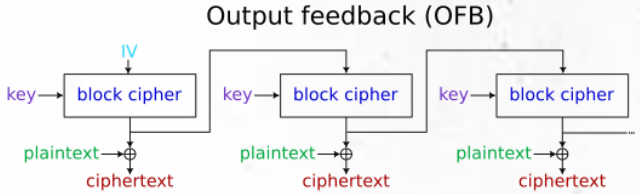
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

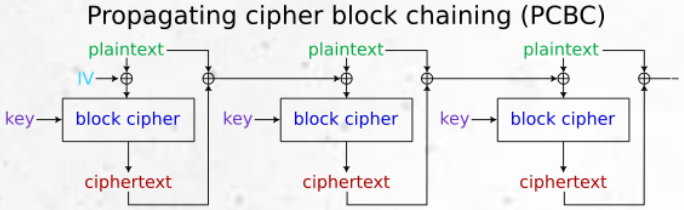
Režimy blokových šifier

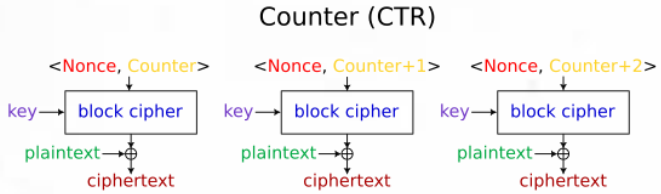




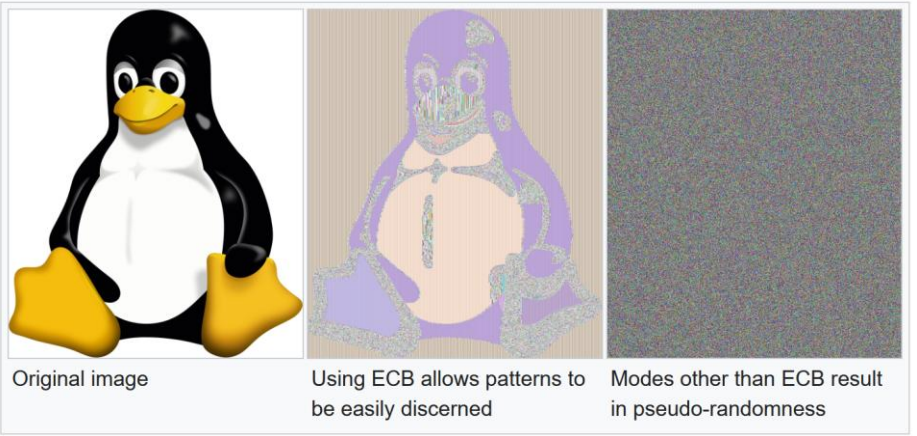








https://upload.wikimedia.org/wikipedia/commons/e/ef/BlockCipherModesofOperation.svg



https://upload.wikimedia.org/wikipedia/commons/9/96/Tux_encrypted_ecb.png

padding – doplnenie do veľkosti bloku

- *pkcs7* *(...03 03 03)*
- *iso7816* *(...80 00 00)*
- *x923* *(...00 00 03)*

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS
UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Asymetrické algoritmy

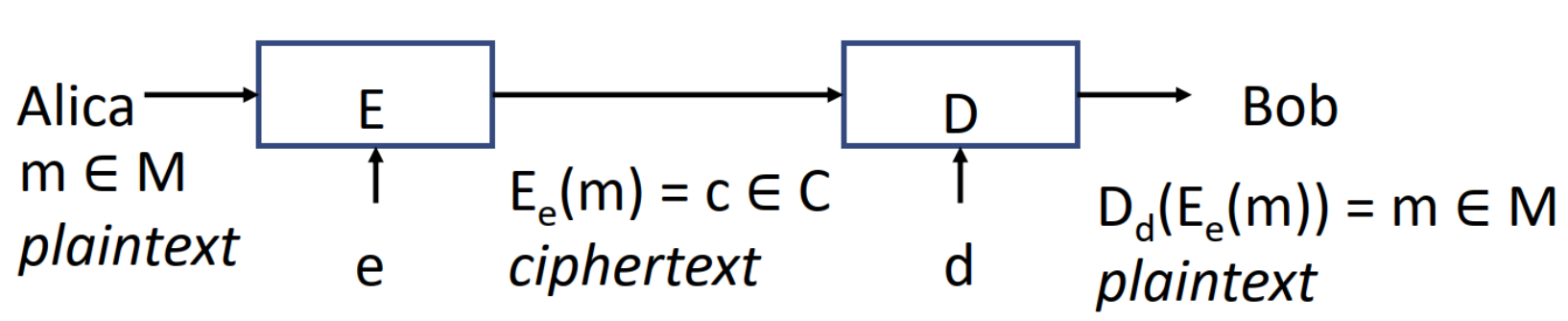
Kryptografické systémy s verejným kľúčom

symetrické šifrovanie – problém s kľúčmi (exponenciálny rast)

asymetrické šifrovanie – rozdelenie kľúča na 2 časti

e – verejný kľúč (public key) Boba (šifrovací)

d – súkromný kľúč (private key) Boba (dešifrovací)



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Princíp asymetrickej kryptografie

pre šifrovaciu funkciu E(e, m) = c je výpočet inverznej funkcie $E^{-1}(e, c) = m$ výpočtovo (algoritmicky dokázateľne) zložitý – jednocestná resp. jednosmerná funkcia (one-way)

na dešifrovanie existuje funkcia $D(d, c) = E^{-1}(e, c) = m$

„zadné vrátka“ (trapdoor) – len ak poznáme d

z e nie je možné jednoducho vypočítať d

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

RSA

Rivest, *Shamir*, *Adleman* (1977)

$n = p.q,\ \phi(n) = (p-1).(q-1),\ e < \phi(n),\ d = e^{-1} \pmod{\phi(n)}$

- súkromný kľúč d, $\phi(n)$, p, q
- verejný kľúč n, e

$E_{n,e}(m) = m^e \bmod n = c$

$D_{n,d}(c) = c^d \bmod n$

p=7, q=13, n = p.q=91, e=5
$\phi(n)$ = (p-1).(q-1) = 6.12 = 72
$d = e^{-1} \equiv 29$

m = 3:
$c = m^e = 3^5 = 243 \equiv 61 \pmod{91}$
$m = c^d = 61^{29} \equiv 3 \pmod{91}$

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ElGamal

ElGamal (1985)

$$e = g^d \pmod p$$

- súkromný kľúč d, $\phi(n)$, p, q
- verejný kľúč p, g, e

$E_{p,g,e}(m) = [g^k \bmod p, (e^k.m) \bmod p] = c$, k - náhodné

$D_{p,g,d}(c) = s.r^{-d} \bmod p$

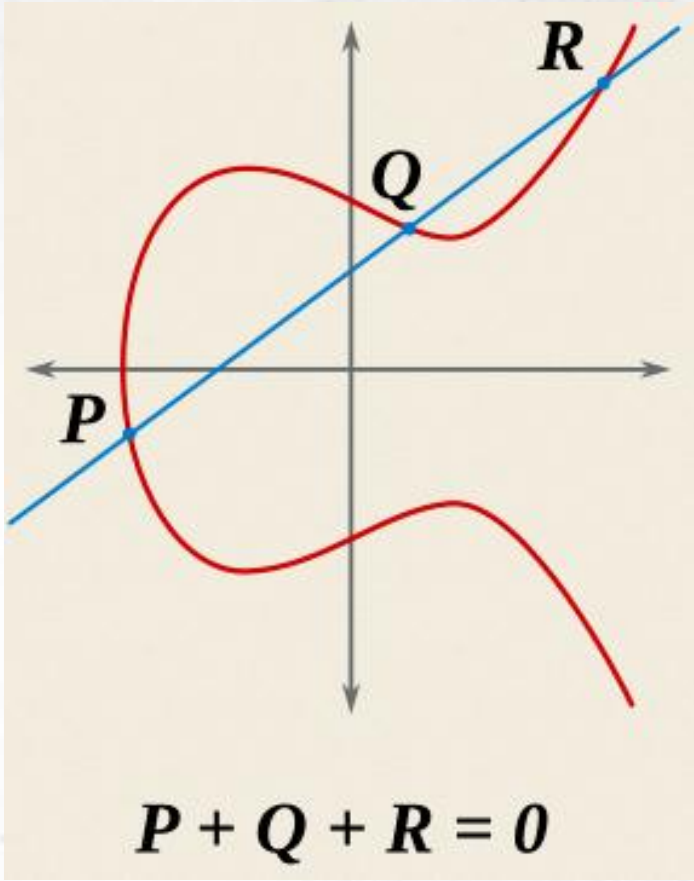
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Eliptické krivky

- 1985 Neal Koblitz, Victor S. Miller
- 1999 NIST F_p, F_{2^n}
- riešenia integrálnych rovníc pre výpočet osí elíps
- všeobecne v tvare

  $y^2 + a.x.y + b.y = x^3 + c.x^2 + d.x + e$
- v kryptografii

  $y^2 = x^3 + a.x + b, (4a^3 + 27b^2 \neq 0)$



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ekvivalentné dĺžky kľúčov

NIST SP 800-57

NIST Special Publication 800-57 Part 1

Revision 5

Recommendation for Key Management

Security Strength	Symmetric Key Algorithms	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
≤ 80	2TDEA	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA[68]	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Dnes sa šifruje symetricky

kľúčom dohodnutým asymetrickou šifrou

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Postkvantová kryptografia

faktorizáciu, DLP, ECDLP je možné riešiť polynomiálne pomocou kvantových počítačov (Shorov algoritmus)

postkvantová kryptografia - založená na problémoch s ťažkým riešením aj s použitím kvantových počítačov

- problémy v mrežových bodoch n-rozmerných priestorov
- lattice-based cryptography, LWE – learning with errors
- ring learning with errors (Ring-LWE)
- NTRU encryption (N-th degree truncated polynomial ring)
- multivariačná kryptografia
- kryptografia na báze autokorekčných kódov (McEliece)
- supersingulárne eliptické krivky

ML-KEM Kyber (512/768/1024 B)
CRYSTALS-Kyber (1632/800 B)
CRYSTALS-Dilithium (2528/1312 B)
SPHINCS
FALCON

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Hešovacie funkcie

- integrita (celistvosť) správy – či nebola urobená zmena počas prenosu (uloženia) - šifrovacie systémy zmeny neriešia ...
- správa ľubovoľnej dĺžky => charakteristický odtlačok pevnej dĺžky (fingerprint, message digest)
- hešovacia funkia (hash) – obyčajné zobrazenie h: $\{0,1\}^* \rightarrow \{0,1\}^n$
- kryptografická hešovacia funkcia (aby ju bolo možné využiť na zabezpečenie integrity správ)

  ťažko invertovateľná, odolná voči nájdeniu druhého vzoru, odolná voči kolíziám

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Hešovacie funkcie

- MD5 (1991 Rivest) 128bit, 4 kolá, kolízie od 2008

  `09e5d37404e113060c4c23148fc6dd64`

- SHA-1 (1995 NSA) 160bit, 4 kolá, kolízie od 2017

  `3b0bbd7b8aaa489bd129ab868a72c2959a43d81b`

- SHA-2 (2001 NSA) 224/256/384/512bit, 64 kôl, *bitcoin*

  `668a6c9f0bafdf9f8fe77e4f56aceb700f30e9a02e24b07796228cd3ea7f6b28`

- SHA-3 (2015) 224/256/384/512, 24 kôl

  `6978683b763a0b9e4a0fa97600a29c5537761283168382216c4d7207cc6465b2`

- Whirlpool (2003) 512bit

  `e18ab746f51a0f64419b528465f10eb00ad6b72136c235cd66cd84942d8e284d`
  `13755cf4949ca4678909ff2967fe7cab5ac47624a49249293f27fa99f7c51a01`

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnostné ciele budovania informačnej bezpečnosti

bezpečnostné ciele, dosahované použitím kryptografických systémov a bezpečnostných mechanizmov ISO/IEC 27000

- dôvernosť (data confidentiality) = šifrovanie (asymetrická, symetrická kryptografia, blokové, prúdové šifry)
  dôvernosť spojenia, jednotlivého bloku, časti správy, toku dát
- celistvosť (data integrity) = integritné schémy (MDC funkcie)
  možnosť opravy, integrita časti správ, detekcia zámeny (replay)
- pôvodnosť (data authentication) = autentifikačné postupy (MAC funkcie)
  pôvodnosť zdroja, identita komunikujúcich
- nepopierateľosť (nonrepudiation) = digitálne podpisovacie schémy
  nepopierateľnosť odosielateľa, príjemcu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Podpisovacie schémy

- asymetrickú kryptografiu je možné použiť na podpisovanie
  - z dokumentu sa vypočíta heš
  - súkromným kľúčom sa zašifruje heš
  - tento zašifrovaný podpis sa priloží k dokumentu
- overenie podpisu
  - vypočíta sa heš dokumentu
  - dešifruje sa heš z podpisu
  - obe hodnoty sa porovnajú

RSA
ElGamal
DSA (Digital Signature Algorithm)
ECDSA (ECC)
EdDSA (Edwards Curve)
ML-DSA (CRYSTALS-Dilithium)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Autentifikácia a autorizácia

identita – faktor identifikujúci jednoznačne osobu/zariadenie

znalosť (heslo)

vlastníctvo (preukaz, telefón, hw kľúč)

vlastnosť (biometria)

Ukladanie hesiel:

- otvorený text
- heš
- heš s náhodným reťazcom (soľou)
- viacnásobný heš

scrypt
bcrypt
Argon2
Balloon

autentifikácia resp. autentizácia (authentication) – preukázanie požadovaných faktorov identity v danom čase daným spôsobom

dvoj-/viac- faktorová

autorizácia – oprávnenie využiť službu, pristúpiť k objektu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Distribúcia verejných kľúčov

Dohoda na kľúči

- A3/A8 (GSM autentifikácia)
- Kerberos (ticket-ovací systém)

  authentification server, ticket grantig server, service server
- Diffie-Hellmann

  „namiešanie“ kľúča

  (súkromný kľúč jednej strany a verejný kľúč druhej strany)
- Encrypted Key Exchange

  zdieľané heslo

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Certifikát

Ako sa ktokoľvek dozvie verejný kľúč Boba?

autenticita (pôvodnosť) verejných kľúčov

reťaz dôvery – prostredníctvom dôveryhodného verejného kľúča dôveryhodného subjektu

dôveryhodná autorita potvrdí verejný kľúč subjektu digitálnym podpisom správy, obsahujúcej verejný kľúč a identitu subjektu

certifikát – spája identitu subjektu s jeho verejným kľúčom

bezpečná distribúcia verejných kľúčov je základ súčasnej kryptografie

certifikáty udeľuje dôveryhodná Certifikačná autorita

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Certifikát (www.upjs.sk)

Certificate

upjs.sk | GEANT TLS RSA 1 | HARICA TLS RSA Root CA 2021

Subject Name

Common Name	upjs.sk

Issuer Name

Country	GR
Organization	Hellenic Academic and Research Institutions CA
Common Name	GEANT TLS RSA 1

Validity

Not Before	Mon, 17 Nov 2025 06:36:29 GMT
Not After	Tue, 17 Nov 2026 06:36:29 GMT

Subject Alt Names

DNS Name	upjs.sk
DNS Name	www.upjs.sk

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	86:3F:B1:E8:14:0F:95:5D:1F:85:E8:2B:8A:98:46:CB:C0:58:AA:DA:2D:1C:10:E7:DB:...

Miscellaneous

Serial Number	0C:DD:31:AC:49:22:57:02:4B:12:24:B8:DD:BD:2D:89
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	8B:61:5A:D3:D1:37:5C:B0:D1:A7:DB:21:6B:91:73:D0:5C:3E:F2:7C:9D:2F:6B:CB:91:...
SHA-1	E8:32:53:C2:96:E3:35:68:AE:7D:66:6B:B1:08:9A:D9:30:48:0B:3A

Key Usages

Purposes	Digital Signature, Key Encipherment

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Životný cyklus certifikátu X.509

- žiadosť a registrácia (registračná autorita)
- vydanie certifikátu
- platnosť

  obnovenie (renew, rekey),

  vypršanie platnosti (exspirácia),

  odvolanie (revokácia)

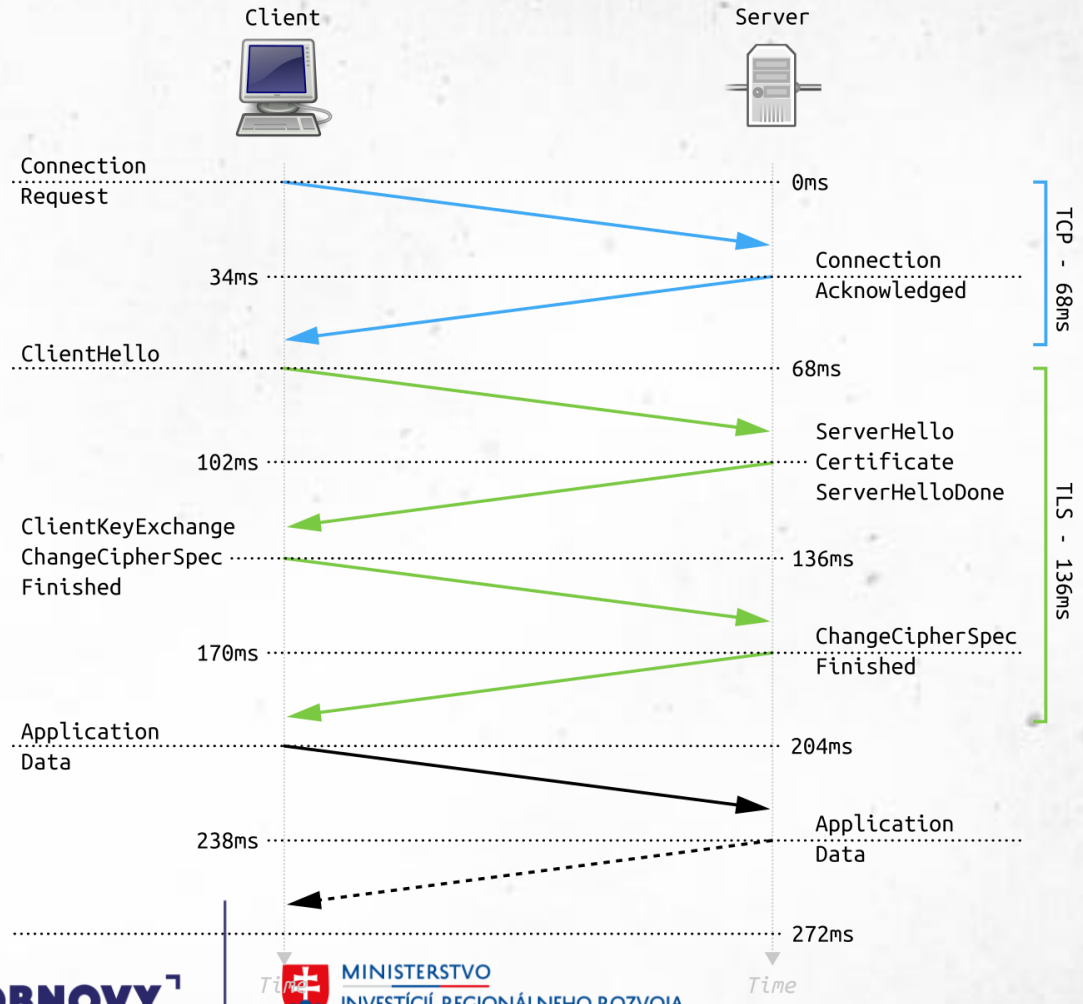
    CRL – zoznam odvolaných certifikátov

    OCSP – online overenie certifikátu
- archivácia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prenos kľúča asymetrickou kryptografiou

- **Transport Layer Security**
  - nástupca SSL 3.0
  - verzia 1.2 (2008)
  - verzia 1.3 (2018)



https://upload.wikimedia.org/wikipedia/commons/d/d3/Full_TLS_1.2_Handshake.svg

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Dohoda na kľúči

perfect forward secrecy

- kompromitácia dlhodobých nespôsobí prezradenie dočasných kľúčov
  - STS (Station-to-Station) – Diffie-Hellmann s obojstrannou autentifikáciou (certifikátmi)

Key Encapsulation Mechanism

- bezpečné vytvorenie a prenos krátkeho symetrického kľúča medzi dvoma stranami cez verejný kanál, kde odosielateľ použije príjemcov verejný kľúč

prenos kľúča kvantovou kryptografiou

- prenos fotónov – polarizované vlnenie – cez polarizačný filter buď prejde celý, alebo neprejde vôbec

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť


meno.priezvisko@upjs.sk


https://cyberawareness.sk