Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Základy kryptografie

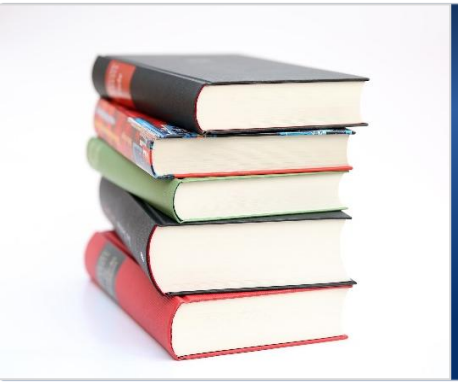
Ochrana dát a súkromia (Blok VII)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti vo verejnej správe

Ing. Ladislav Mariš, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

ladislav.maris@uniza.sk



Obsah

- **Vývoj kryptografie**
- **Symetrická a asymetrická šifra, hashovanie, infraštruktúra verejných kľúčov (PKI)**

Cieľ

- Získať prehľad o základných princípoch a technikách kryptografie, ktoré tvoria základ kybernetickej ochrany dát a komunikácie.

- Rozlišovať medzi **symetrickou** a **asymetrickou šifrou**
- Pochopiť význam a použitie **hashovacích funkcií, šifrovania a dešifrovania**
- Pochopiť úlohu **infraštruktúry verejných kľúčov (PKI)** pri overovaní identity a zabezpečení komunikácie

Praktický význam kryptografie v kybernetickej ochrane

- Kryptografia alebo šifrovanie je veda o metódach **utajovania významu správ ich prevodom do podoby, ktorá je čitateľná len so špeciálnymi znalosťami.**

PRAKTICKY:

- Šifrovanie komunikácie
- Zabezpečenie webstránok
- Digitálne podpisovanie dokumentov
- Ochrana uložených údajov
- Autentifikácia a autorizácia

- Dôverné uchovávanie a prenos informácie
- Chráni pred neautorizovaným prístupom, manipuláciou a únikom dát

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Historické pozadie kryptografie

- Kryptografia existuje už tisíce rokov
  - slúžila na utajovanie správ **v boji či v politike**.
- Výber daní a poplatkov (kupec)
- Hlinené nádoby (predmety, šifry, pečať)
- **Medzi odosielateľom a príjemcom**
- Najskôr mechanické ukrývanie potom šifry
- **Staroveký Egypt** (+2000 p. n. l.)
  - hrobka Khnumhotep II, upravené hieroglyfy
- **Mezopotámia** (+1500 p. n. l.)
  - klinové písmo, rozumeli len zasvätení
- **Grécko** (+ 500 p. n. l.) - transpozícia
  - skytaly, správne natočenie pergamenu/kože na valcovitý tvar s dohodnutým priemerom a dĺžkou, princíp transpozície

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Cézarova šifra (obdobie G. I. Caesara, 100 p. n. l) (úloha)

- Vojenské účely
- **Substitučná šifra**
- Princíp spočíva v nahradení (v posunutí) písmen v abecede, napr. o fixný počet
- n = m-1 (m = počet znakov napr. 46 alebo pridaním ďalších znakov aj viac)
- Zmena smeru: **+n šifrujem** alebo **-n dešifrujem**
- Ak n = 3, potom čo znamená šifra: ÄKMKÓB (písmeno - n)

A	Á	Ä	B	C	Č	D	Ď	DZ	DŽ
E	É	F	G	H	CH	I	Í	J	K
L	Ľ	Ĺ	M	N	Ň	O	Ó	Ô	P
Q	R	Ŕ	S	Š	T	Ť	U	Ú	V
W	X	Y	Ý	Z	Ž				

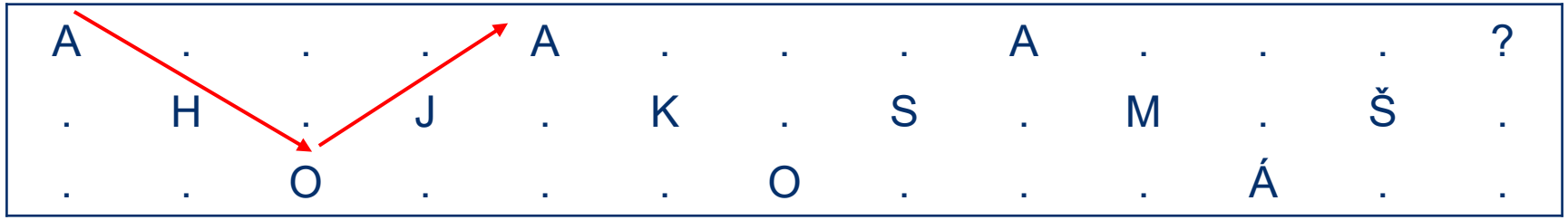
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Transpozícia v šifrovaní

- Transpozícia je typ šifrovania, pri ktorom sa nemenia znaky samotné, ale mení sa ich poradie v správe podľa určitého systému (algoritmu).
- **Znaky správy sa "premiešajú"** podľa kľúča alebo pravidla.
- Výsledkom je šifra, ktorá má rovnaké znaky ako otvorený text, len v inom poradí.
- Napr. **TAJNE** -> **JETNA**
- **Kľúč je: 3-5-1-4-2**

- Jednoduchšie odhalenie permutačnými technikami
- Transpozíciu je lepšie kombinovať so substitúciou pre lepšie výsledky
- Skytala, cikcak šifra (železničný plot)

  AAA?HJKSMŠOOÁ



Atbaš, Frekvenčná analýza, prvé metódy

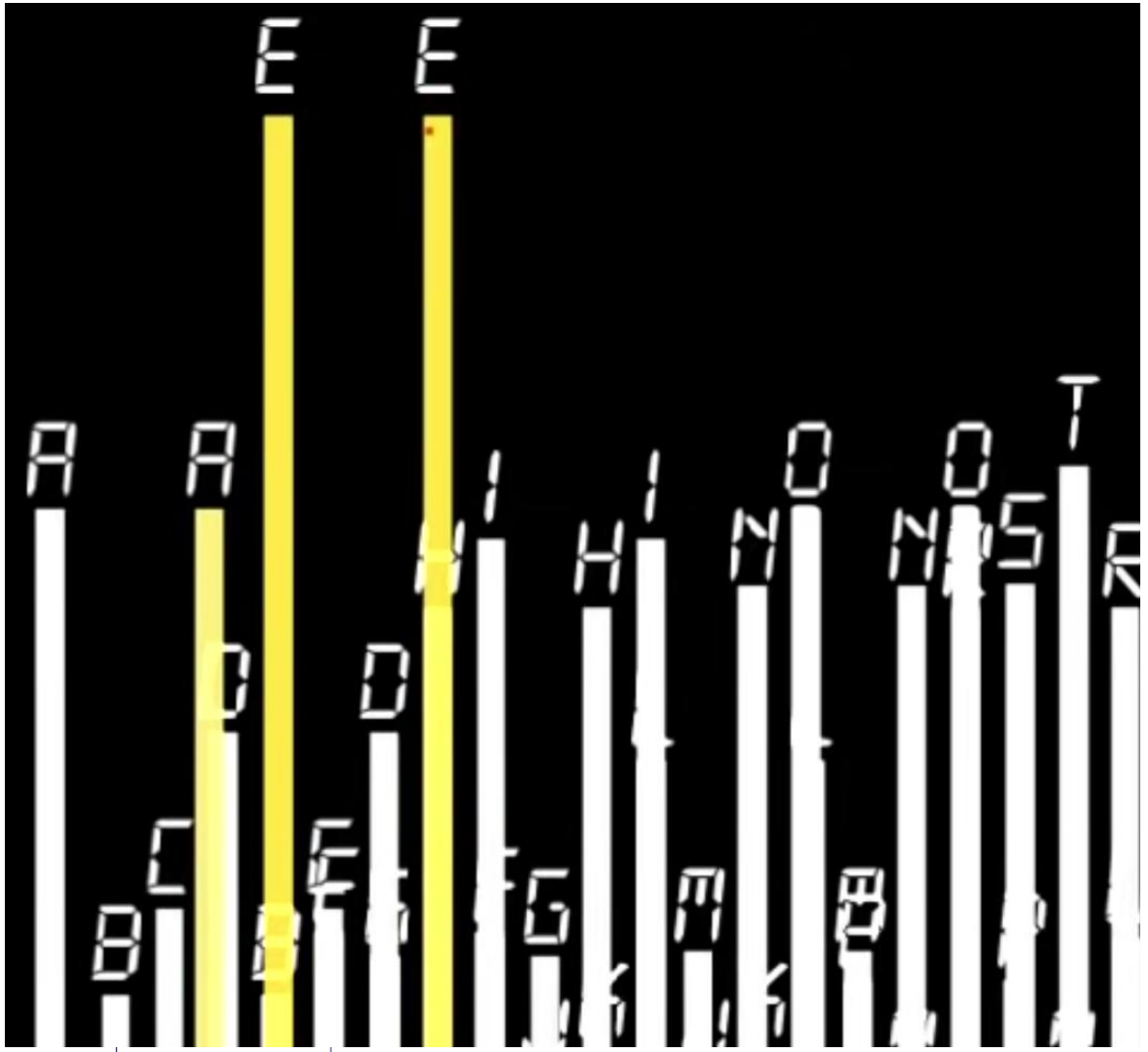
- **Atbaš** (Atbah) (+500 p. n. l. hebrejská substitučná metóda, alef/tav, bet/šin)
  - 1. = n, 2. = n-1; Vychádzalo z hebrejskej abecedy, *pr. šešach* = *babel*, Jeremiáš 25-26
- **Al-Kindí** (801 - 873 n. l.) - arabský filozof, matematik, astronóm, kryptanalýza
  - Vydal dielo: *Rukopis pre dešifrovanie kryptografických správ* (opísal rôzne druhy šifier)
  - **Frekvenčná analýza** - metodika na odhalenie šifrovacích pravidiel na základe frekvencie písmen pomocou spojenia jazykovedy a matematiky
  - všímať si opakujúce sa písmená/slová, porovnávať frekvenciu zašifrovaných slov s frekvenciou jazyka, odhadovať možné slová, skladať hypotézy

- **Al-Qalqashandī** (1355-1418), **Ibn al-Durayhim** (1312-1361) (arabčina, klasifikácia šifrovacích metód, encyklopedické spracovanie šifier, praktické metódy)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Frekvenčná analýza - základný nástroj kryptoanalýzy

- **Opiera sa o štatistické poznatky o jazyku a umožňuje odhaliť pôvodný (otvorený) text na základe toho, ako často sa v jazyku vyskytujú jednotlivé písmená alebo ich kombinácie.**
- Prirodzené jazyky totiž nevykazujú rovnomerné rozloženie znakov.
- Jej účinnosť sa najviac prejavuje pri **klasických substitučných alebo transpozičných šifrách**, ktoré iba nahrádzajú znaky inými znakmi bez zmeny ich celkového rozloženia.
- https://www.matweb.cz/frekvencni-analyza/



Polyalfabetické šifrovanie (neskôr rotorový systém)

- **Leon Batista Alberti** (1404-1472) bol taliansky polyhistor a považuje sa spolu s Johanessom Trithemiusom (1462 – 1516) za zakladateľov európskej kryptografie
- Alberti v roku 1467 vynašiel novú techniku, dnes známu ako **polyalfabetické šifrovanie**, ktorá využívala výhodu používania **viacerých substitučných abecied** namiesto jednej.
- Zároveň vytvoril jednoduchý spôsob, ako **generovať množstvo rôznych substitučných vzorov** počas jednej komunikácie.
- Dve strany si najprv vymenili **malé množstvo informácií** (tzv. **kľúč**), na základe ktorého potom **vytvorili viacero abecied**.
- Každé písmeno otvoreného textu sa tak mohlo zašifrovať pomocou inej substitúcie v rámci jednej správy.
- Táto myšlienka bola **jednoduchá a veľmi efektívna**, no v praxi sa ukázalo, že jej správne použitie bolo náročnejšie, ako sa pôvodne predpokladalo.
- Mnohé šifry, ktoré na Albertiho koncepte stavali, boli iba **neúplnými implementáciami** a preto sa dali **relatívne ľahko prelomiť** – ako napríklad neskôr **Vigenèrova šifra**.

Ilustrácia Albertiho disku
otáčanie menšieho disku na stabilnom väčšom disku
Každé nové otočenie znamená **novú substitučnú abecedu** – **polyalfabetická substitúcia**
Tajný kľúč obsahuje inštrukcie, ako a kedy disk posúvať

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Vigenèrova šifra (16. storočie)

- **Blaise de Vigenère** (1523–1596) – francúzsky diplomat
- Vytvoril **polyalfabetickú** šifru, ktorá bola považovaná za nerozlúštiteľnú (do 19.st)
- Polyalfabetická substitučná šifra – **každé písmeno/slovo/veta správy je šifrované inou abecedou**, bráni frekvenčnej analýze, pretože rovnaké písmená môžu byť zašifrované rôzne

A 0	Á 1	Ä 2	B 3	C 4	Č 5	D 6	Ď 7	DZ 8	DŽ 9
E 10	É 11	F 12	G 13	H 14	CH 15	I 16	Í 17	J 18	K 19
L 20	Ľ 21	Ĺ 22	M 23	N 24	Ň 25	O 26	Ó 27	Ô 28	P 29
Q 30	R 31	Ŕ 32	S 33	Š 34	T 35	Ť 36	U 37	Ú 38	V 39
W 40	X 41	Y 42	Ý 43	Z 44	Ž 45				

- **ŽILINA**
- použijeme **kľúč**: **ŠIFRA**
- dĺžka slova ŽILINA = 6 písmen -> ŠIFRAŠ **->** **SŔŔÁNŠ**
- ak použijeme vybranú abecedu, potom každé písmeno v danej abecede má svoju pozíciu napr. písmeno **Ž** = 45 a písmeno **Š** = 34 (indexujeme od 0)
- súčet je 79; potom 79 % len(abeceda) = index[33] = **S** (zvyšok po delení 46 znakov), v programovaní by sme získali iný výsledok v dôsledku dvojznakovej abecedy (dz,dž,ch)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Vigenèrova šifra / šifrujeme a dešifrujeme (úloha)

Pôvodný	+	Kľúč	=	Súčet	mod 46	Výsledok
Ž (45)	+	Š (34)	=	79	33	S
I (16)	+	I (16)	=	32	32	Ŕ
L (20)	+	F (12)	=	32	32	Ŕ
I (16)	+	R (31)	=	47	1	Á
N (24)	+	A (0)	=	24	24	N
A (0)	+	Š (34)	=	34	34	Š

Šifrovaný	-	Klúč	=	Rozdiel	mod 46	Výsledok
33 (S)	-	Š (34)	=	-1	45	Ž
32 (Ŕ)	-	I (16)	=	16	16	I
32 (Ŕ)	-	F (12)	=	20	20	L
1 (Á)	-	R (31)	=	16	16	I
24 (N)	-	A (0)	=	24	24	N
34 (Š)	-	Š (34)	=	0	0	A

A 0	Á 1	Ä 2	B 3	C 4	Č 5	D 6	Ď 7	DZ 8	DŽ 9
E 10	É 11	F 12	G 13	H 14	CH 15	I 16	Í 17	J 18	K 19
L 20	Ľ 21	Ĺ 22	M 23	N 24	Ň 25	O 26	Ó 27	Ô 28	P 29
Q 30	R 31	Ŕ 32	S 33	Š 34	T 35	Ť 36	U 37	Ú 38	V 39
W 40	X 41	Y 42	Ý 43	Z 44	Ž 45				

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Wilhelm Kasiski (1805 - 1881)

- Pruský vojenský dôstojník a kryptograf
- "Die Geheimschriften und die Dechiffrir-Kunst"
  (Tajné písma a umenie dešifrovania)

Kasiskiho test (1854)

- Prvá systematická **metóda na prelomenie polyalfabetických šifier (prelomenie Vigenèrovej šifry)**
- Pozorovanie **opakujúcich sa sekvencií znakov** v šifrovanom texte
- Výpočítame vzdialenosť medzi opakovaniami a tým **odhadneme dĺžku kľúča** = (opakovaná sekvencia znakov), výpočítame najväčšiho spoločného delitela (dĺžka klúča), následne podľa dĺžky klúča sa rozdelil text na bloky
- Po určení dĺžky sa na každý blok textu mohla použiť frekvenčná analýza

William F. Friedman (1891–1969)

- Americký vojenský spravodajský kryptograf, vedec
- Patrí medzi zakladateľov modernej kryptanalýzy
- Vytvoril metódu: index koincidencie a "*otvoril dvere*" modernej kryptografii

Friedmanov index (test) koincidencie (1920 +-) + Babbage

- Štatistická metóda na určenie dĺžky kľúča v polyalfabetických šifrách (Vigenère)
- Rozlišujeme medzi rôznymi typmi šifrovania s rozpoznaním jazyka
- *V bežných jazykoch sa niektoré písmená (E v angličtine alebo A v slovenčine) vyskytujú častejšie*
- Index koincidencie meria **pravdepodobnosť,** že náhodne vybrané dva znaky budú rovnaké
- **Friedman** použil **štatistiku a jazykové zákonitosti**, aby prelomil zložité šifry.
- **Index koincidencie** dnes patrí k základným nástrojom v kryptanalýze.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Index koincidencie

- Jeden zo základných nástrojov šifrovania/dešifrovania
- *Koincidencia* (zhoda, výskyt 2+ javov súčasne)
- Pravdepodobnosť, že **dva náhodne vybrané znaky z textu budú rovnaké**
- *Zistíme či text je šifrovaný monoalfabeticky alebo polyalfabeticky*
- *Určíme jazyk textu (typ jazyka)*
- *Mohli by sme odhadnúť aj dĺžku kľúča*
- **IoC blízko 0.07** → prirodzený text (alebo monoalfabetická šifra)
- **IoC blízko 0.038** → náhodný text (alebo polyalfabetická šifra s dlhým kľúčom)
- **Nižší IoC** = vyššia entropia = ťažšie identifikovateľné písmená = pravdepodobne šifrovaný text
  - *Text **„AAAAAA“** má IoC = 1 (všetky znaky sú rovnaké)*
  - *Text **„ABCDEFG“** má IoC blízko 0 (žiadne dva znaky nie sú rovnaké)*
- Pre text s dĺžkou **N** a s počtami jednotlivých písmen $\mathbf{n_1}$, $\mathbf{n_2}$, ..., $\mathbf{n_k}$ platí:

Text / jazyk	Približná hodnota
Slovenčina	~0.070
Angličtina	~0.068
Francúzština	~0.077
Náhodný text	~0.038

$$\mathrm{IoC} = \frac{\sum n_i(n_i - 1)}{N(N-1)}$$

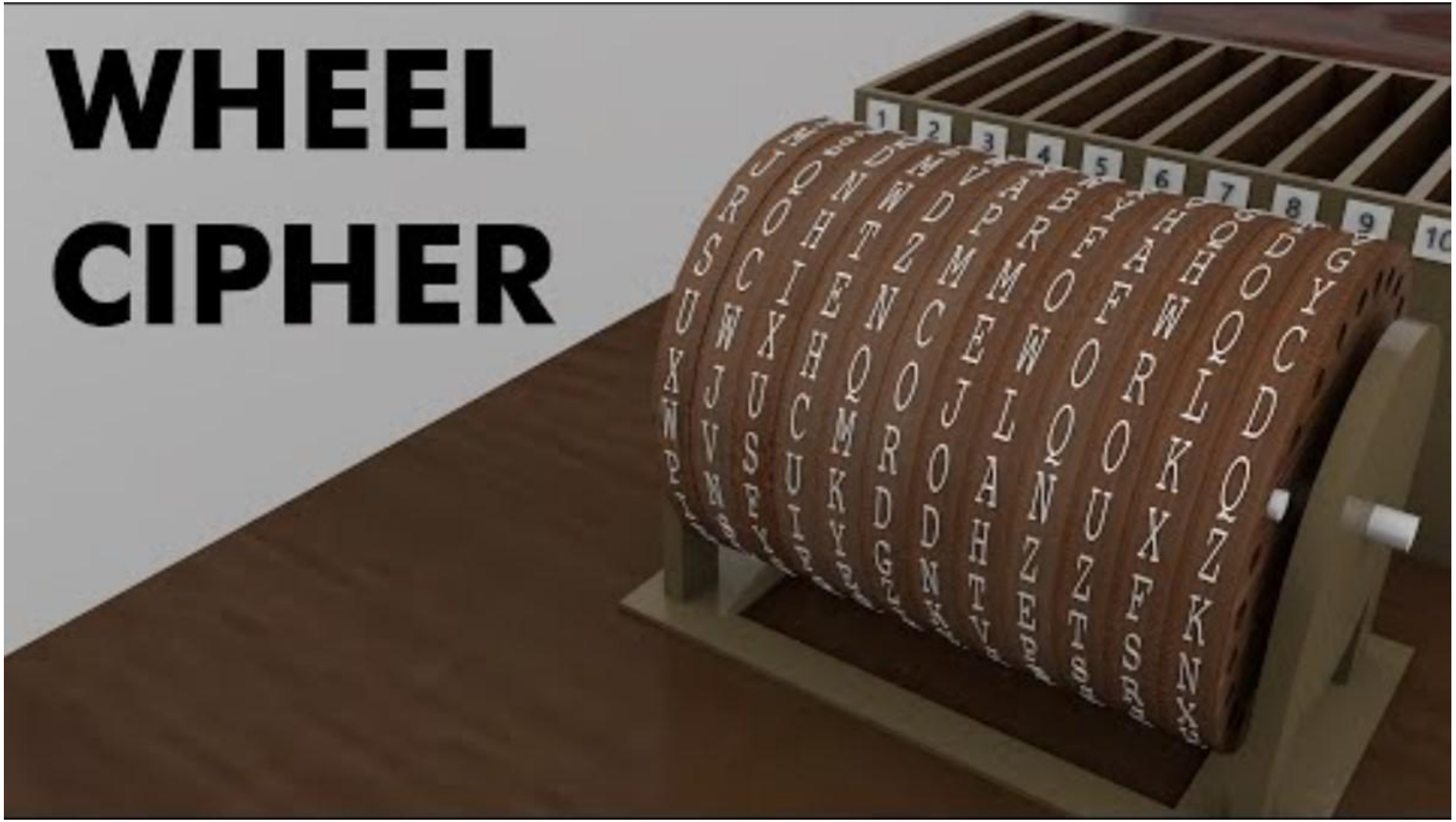
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Mechanické šifrovanie Prechod od ručného šifrovania k mechanickému

- **Thomas Jefferson** (1743 - 1826) - 3. prezident USA
  (v roku 1789 opísal systém rotujúcich kotúčov, nevyrobil ho, rukopis *znovunašli* v 1922, T. J. považoval za praktickejší iný systém - *stĺpcová transpozičná šifra*)
- **zväzok otáčajúcich sa diskov na osi s rôznym usporiadaním písmen po obvode**
- **Jeffersonov disk 1789 (36** až 48 kotúčov**)**
- **Etienne Bazerie (vojenský kryptograf) (cca 1890-1901)**
  - **Bazerieho valec (cylinder), francúzska armáda (20 kotúčov)**
- **kolesová šifra**
- **Rotujúce kotúče s písmenami (*kombinovaný zámok*)**

- Prvý prototyp na báze Jeffersonovho disku vynašiel švédsky barón **Fredrik Gripenstein** (1786) - 57 diskov na nahradenie písmen zadaných úradníkom na jednej strane zariadenia a na druhej strane zariadenia viditeľnými pre úradníka

Jeffersonov disk – video (kolesová, disková šifra)



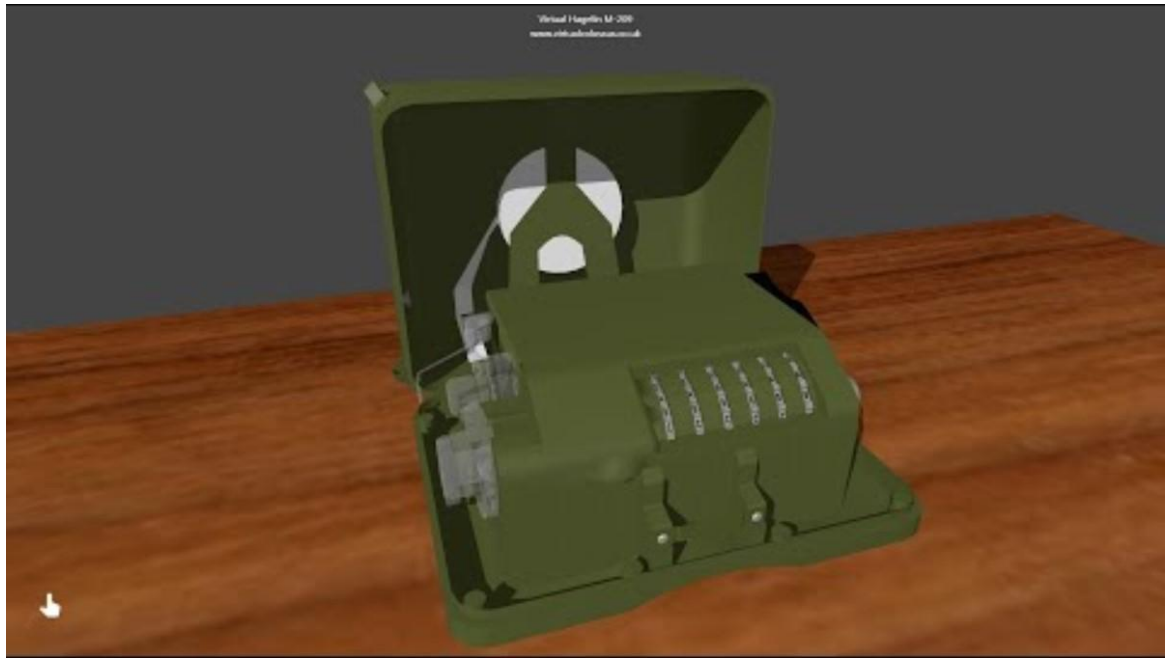
M-94 (1922 – 1943)

- **(elektro) mechanické šifrovacie** zariadenie vyvinuté pre armádu USA
- 25 otočných diskov, každý s náhodne usporiadanou abecedou
- Disky boli navlečené na spoločnej osi – podobne ako Jeffersonov disk
- **Poradie diskov bolo tajným kľúčom na šifrovanie a dešifrovanie**
- Každý disk sa nastavil podľa písmen správy a z iného riadku na diskoch sa potom čítala **zašifrovaná verzia správy**
- **Dešifrovanie**:
  rovnaké nastavenie diskov,
  čítanie správneho riadku

M-209 (nadviazal na C-35, C-36...)

- Vojenský kryptografický stroj, využívaný počas 2. s.v. aj počas vojny v Kórei
- Boris Hagelin 1892 – 1983 - švédsky vynálezca šifrovacieho stroja C-35/36, resp. M-209
- Stroj M-209 bol prenosným mechanickým šifrovacím strojom
- Bez elektriny - vhodný na bojiská
- Komplexný polyalfabetický stroj

- Patrí do kategórie **rotorových šifrovacích strojov** (Alberti, …., Hengel, Hebern, **A. Scherbius**) - elektromechanický stroj na šifrovanie/dešifrovanie pomocou polyalfabetických šifier (ručné operácie trvali dlho), každé písmeno sa mohlo šifrovať podľa iného nastavenia, 20. – 70. roky 20. st,)



Video: Rotorový šifrovací stroj M-209

Rotorový stroj - princíp fungovania

1. Každý rotor obsahuje vnútornú prepojenú abecedu – každé písmeno je prepojené na iné písmeno.
2. Keď zadáte písmeno, **elektrický prúd alebo mechanický pohyb** prejde cez rotory, pričom sa písmeno transformuje podľa vnútornej prepojky.
3. Po každom stlačení klávesu sa prvý rotor otočí o jeden krok (ako počítadlo).
4. Po celom otočení prvého rotora (napr. po 26 stlačeniach) sa otočí druhý rotor, potom tretí a tak ďalej (podobne ako ručičky hodín).
5. Každý stisk klávesu preto spôsobuje, že cesta signálu cez rotory je iná než predchádzajúca – šifrovanie sa dynamicky mení.
6. Rôzne natavenia diskov, veľkostí, počtu písmen, spôsobov otočenia, ...

Enigma - elektromechanická polyalfabetická substitúcia (dynamická)

Enigma bol **elektromechanický šifrovací stroj**, ktorý sa používal na šifrovanie a dešifrovanie správ. Najznámejšia je jeho vojenská verzia, ktorú nacistické Nemecko používalo počas 2. svetovej vojny. Mala 10^{23} možných kombinácií. Nastavenie stroja sa menilo každý deň. Vynálezca **Arthur Scherbius v roku 1918**.

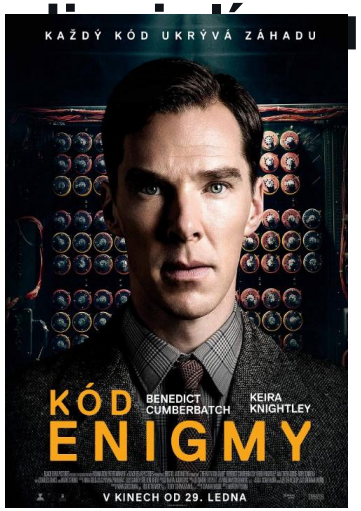
1. **Klávesnica**:
   Používateľ zadal písmeno (napr. „A“).
2. **Rotory (kolesá, disky)**:
   Elektrický prúd prešiel cez niekoľko **otáčajúcich sa rotorov**, pričom **každý rotor menil elektrickú cestu**.
3. **Reflektor (odrazka)**:
   Na konci prúd narazil na **reflektor**, ktorý ho poslal späť inou cestou cez rotory.
4. **Výstup**:
   Nakoniec sa rozsvietila **žiarovka s iným písmenom** (napr. "G"), ktoré predstavovalo šifrovaný znak.
5. **Dynamika**:
   Po každom stlačení klávesu sa **rotory automaticky posunuli**, čím sa zmenilo šifrovanie pre nasledujúce písmeno.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Enigma - video

Prelomenie Enigmy (Lorentz) a nástup počítačov

- Prelomenie na základe matematickej analýzy, teórie permutácii (štatistiky), logiky a výkonných strojov (Marian Rejewski a Alan Turing; stroje Bombe, Collosus (1943) – predchodca moderných počítačov na báze dierovaných papierovýsh pásov, Mark I, Mark II, ...)
- Potreba matematicky overenej bezpečnosti: **kryptografia sa stáva matematickou**
- Predznamenia vývoja počítačov
- Zrodenie informačnej bezpečnosti
- Základy kyberbezpečnosti



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Binárne XOR maskovanie (šifrovanie)

- XOR (exclusive OR) maskovanie je jednoduchá, ale silná technika na šifrovanie dát, kde pôvodný text a kľúč kombinujeme bit po bite pomocou operácie XOR s inými dátami.
- **Ak sú bity rovnaké**, výsledok je **0**.
- **Ak sú bity rôzne**, výsledok je **1**.
- Ak je **kľúč kvalitný a náhodný**, šifra je **prakticky neprelomiteľná**.
- Ak je **kľúč predvídateľný alebo sa opakuje**, šifra je **zraniteľná** (ako napríklad Enigma, keď opakovali kľúče).

Bit 1 (správa)	Bit 2 (tajný kľúč)	Výsledok XOR
0	0	0
0	1	1
1	0	1
1	1	0

XOR šifrovanie/maskovanie šifrovania

- **Krok 1: Prevod znaku na bity**
  - Písmeno **A** v ASCII kódovaní je číslo **65**. V binárnej forme je to: A = 01000001
- **Krok 2: Operácia**

"A"	0	1	0	0	0	0	0	1
Kľúč	1	0	1	0	1	0	0	0
Správa	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**1**

Bit 1 (správa)	Bit 2 (tajný kľúč)	Výsledok XOR
0	0	0
0	1	1
1	0	1
1	1	0

- **Krok 3: Binárne číslo 11101001 = 233 = Ú**
- **Krok 4: Dešifrujem Ú s rovnakým kľúčom**

"Ú"	1	1	1	0	1	0	0	1
Kľúč	1	0	1	0	1	0	0	0
Správa	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**

Enigma vs. Lorentz

Vlastnosť	Enigma	Lorenz SZ40/SZ42
Účel	Taktičná komunikácia (polné jednotky)	Strategická komunikácia (nacisti, generálne štáby)
Typ šifrovania	**Polyalfabetická substitučná šifra**	**Binárne XOR** maskovanie teletypových správ (písané správy na diaľku, predchodza emailu)
Pracovalo s	**Písmenami (A–Z)**	**Binárnymi dátami (0 a 1)**
Počet rotorov/kolies	3 až 4 rotory	12 kolies (5 chi, 5 psi, 2 motorové kolieska)
Komplexnosť	Vysoká (milióny nastavení)	Extrémne vysoká (kvadrilióny možností)
Mechanizmus	Elektricko-mechanický (svetielka, klávesnica)	Elektromechanický (papierové pásy, binár signály)
Prenos správ	Ručne, papierovo	Automatizovane cez teletype
Prelomenie	Marian Rejewski, Alan Turing a tím v Bletchley Park	Bill Tutte, Tommy Flowers, Colossus v Bletchley Park
Význam prelomenia	Skrátenie vojny o 2–4 roky	Zachytávanie strategických plánov nacistického velenia
Technológia prelomenia	Bombe (elektromechanické zariadenie)	Colossus (prvý elektronický počítač)

Elektronizácia a automatizácia šifrovania po 2. sv. vojne

- Po vojne vznikali nové šifrovacie zariadenia založené na elektronike (už nie iba na mechanike a relé). Vývoj sa preniesol aj do studenej vojny (najmä USA, VB, Sovietsky zväz).
- Kryptografia sa presúva zo špecializovaných zariadení (napr. Enigma) **do softvérových riešení**, ktoré bežia na univerzálnejších počítačoch (EDSAC, UNIVAC)
- Vývoj šifrovacích štandardov na vojenské, diplomatické a civilné účely (70. roky)
- V 50. a 60. rokoch sa kryptografia stala doménou veľkých štátnych inštitúcií, ako napríklad **NSA** v Spojených štátoch, ktoré vyvíjali sofistikované, ale utajené systémy šifrovania.
- Kryptografia bola považovaná za výsostne vojenskú a vládnu oblasť, kde bola snaha udržať všetky pokroky mimo dosahu verejnosti.

Moderné obdobie 1970´ - súčasnosť

- Skutočný prelom však nastal v 70. rokoch 20. storočia, kedy sa kryptografia postupne otvorila aj civilnému sektoru.
- V roku **1976** predstavili **Whitfield Diffie** a **Martin Hellman** koncept verejného kľúča, ktorý umožnil bezpečnú komunikáciu aj medzi stranami, ktoré si predtým nevymenili tajný kľúč. Tento koncept bol absolútnou revolúciou – umožnil vznik **asymetrickej kryptografie**, kde sa na šifrovanie a dešifrovanie používajú rôzne kľúče.
- V roku **1977**, vznikol **RSA algoritmus** (**R**ivest, **S**hamir, **A**dleman), prvá praktická realizácia kryptografie verejného kľúča a súkromného klúča, ktorý sa používa v elektronickom podpise, online bankovníctve a bezpečnej komunikácii na internete. Princíp veľkých prvočíselných súčinov.
- Ďalším dôležitým krokom bolo zavedenie **DES (Data Encryption Standard)** v roku 1977 ako prvého široko akceptovaného štandardu pre šifrovanie dát. Aj keď bol neskôr prekonaný a nahradený modernejšími štandardmi, ako je **AES (Advanced Encryption Standard)**, DES odštartoval éru **štandardizovanej bezpečnosti** pre civilné aj podnikové využitie.
- Od 90. rokov sa kryptografia stala neoddeliteľnou súčasťou každodenného života:
  - chráni **internetové transakcie**, **e-maily**, **mobily**, **bankové systémy**, **blockchain** a mnoho ďalších oblastí.
- V súčasnosti čelí kryptografia novým výzvam, najmä vďaka **umelej inteligencii a kvantovým počítačom**, ktoré by v budúcnosti mohli prelomiť dnes bežne používané šifry ako RSA alebo ECC (matematika elyptických kriviek).
- Preto sa vyvíja nová generácia algoritmov, známa ako **postkvantová kryptografia**.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Symetrické šifrovanie a Asymetrické šifrovanie

SYMETRICKÉ:

- Používa sa jeden spoločný kľúč, ktorým sa šifruje aj dešifruje.
- Kľúč je ptorebné poznať (odovzdať) ak chceme dešifrovať.

ASYMETRICKÉ:

- Používajú sa dva rôzne kľúče – verejný a súkromný. Verejný kľúč šifruje, súkromný dešifruje.
- Napr. digitálny podpis
- Verejný klúč môže poznať ktokoľvek.

Symetrické vs. Asymetrické šifrovanie

Vlastnosť	Symetrické šifrovanie	Asymetrické šifrovanie
Počet kľúčov	1 (rovnaký kľúč na šifrovanie aj dešifrovanie)	2 (verejný a súkromný kľúč)
Príklady algoritmov	**AES**, DES, 3DES, RC4, Blowfish	**RSA**, ECC, DSA, ElGamal
Rýchlosť spracovania	Veľmi rýchle	Pomalšie (náročné na výpočty)
Bezpečnosť prenosu kľúča	Riziko (kľúč treba bezpečne odovzdať)	Bezpečnejšie (verejný kľúč môže poznať každý)
Použitie v praxi	Šifrovanie veľkých súborov, diskov, komunikácie (VPN, Wi-Fi)	Výmena kľúčov, digitálne podpisy, certifikáty
Veľkosť kľúča	Kratšie kľúče (napr. 128 alebo 256 bitov)	Dlhšie kľúče (napr. 2048 alebo 4096 bitov)
Škálovanie na viac užívateľov	Komplikované – každý pár potrebuje vlastný tajný kľúč	Jednoduché – každý má svoj vlastný verejný kľúč
Komplexnosť algoritmu	Jednoduchšie implementácie	Zložitejšie matematiky (napr. prvočísla, eliptické krivky)
Odolnosť voči budúcim hrozbám	Dobrá (pri dostatočne veľkom kľúči)	Citlivejšie na kvantové počítače (potreba postkvantovej kryptografie)
Výhoda	Rýchlosť a efektívnosť pri veľkom objeme dát	Bezpečnosť pri výmene kľúčov cez nezabezpečené kanály
Nevýhoda	Problém bezpečne preniesť tajný kľúč	Pomalšie šifrovanie a dešifrovanie

AES šifrovanie

- **AES (advanced encryption standard)** je moderný symetrický šifrovací algoritmus, ktorý sa používa cca 25 rokov celosvetovo: IB, HTTPS, VPN, WiFi
  - Bloková šifra = šifruje dáta po blokoch s veľkosťou nap. 128 bitov (16 znakov) a používa sa symetrický kľúč napr. AES-256 (256 bitov)
  - Kombinuje rôzne metódy šifrovania
  - https://www.youtube.com/watch?v=C4ATDMIz5wc

AES šifrovanie

AES (Advanced Encryption Standard) je moderný symetrický šifrovací algoritmus, ktorý sa používa na bezpečné šifrovanie dát v blokoch. Každý vstupný blok má veľkosť **128 bitov** (čo zodpovedá 16 bajtom, teda 16 znakom). AES používa **ten istý tajný kľúč** na šifrovanie aj dešifrovanie a patrí medzi najrozšírenejšie algoritmy dnešnej doby.

Počet kôl (rounds), ktorými AES spracováva každý blok, závisí od dĺžky šifrovacieho kľúča: **AES-128** 10 kôl, **AES-192** 12 kôl, **AES-256** 14 kôl.

Ešte pred samotným šifrovaním sa vstupný blok a kľúč rozdelia do tzv. **matice stavu** (state), čo je tabuľka 4x4 bajtov. Každé kolo potom upravuje túto maticu pomocou niekoľkých matematických operácií.

Krok 0: AddRoundKey (prípravná fáza) Ešte pred prvým kolom sa blok XORuje s počiatočným rozšíreným kľúčom. Ide o tzv. **zmiešanie kľúča** (AddRoundKey), ktoré zabezpečí prvotnú transformáciu dát na základe tajného kľúča.

Krok 1 až N: Hlavné kolo šifrovania: Každé kolo pozostáva zo štyroch operácií (okrem posledného kola, ktoré má len tri):

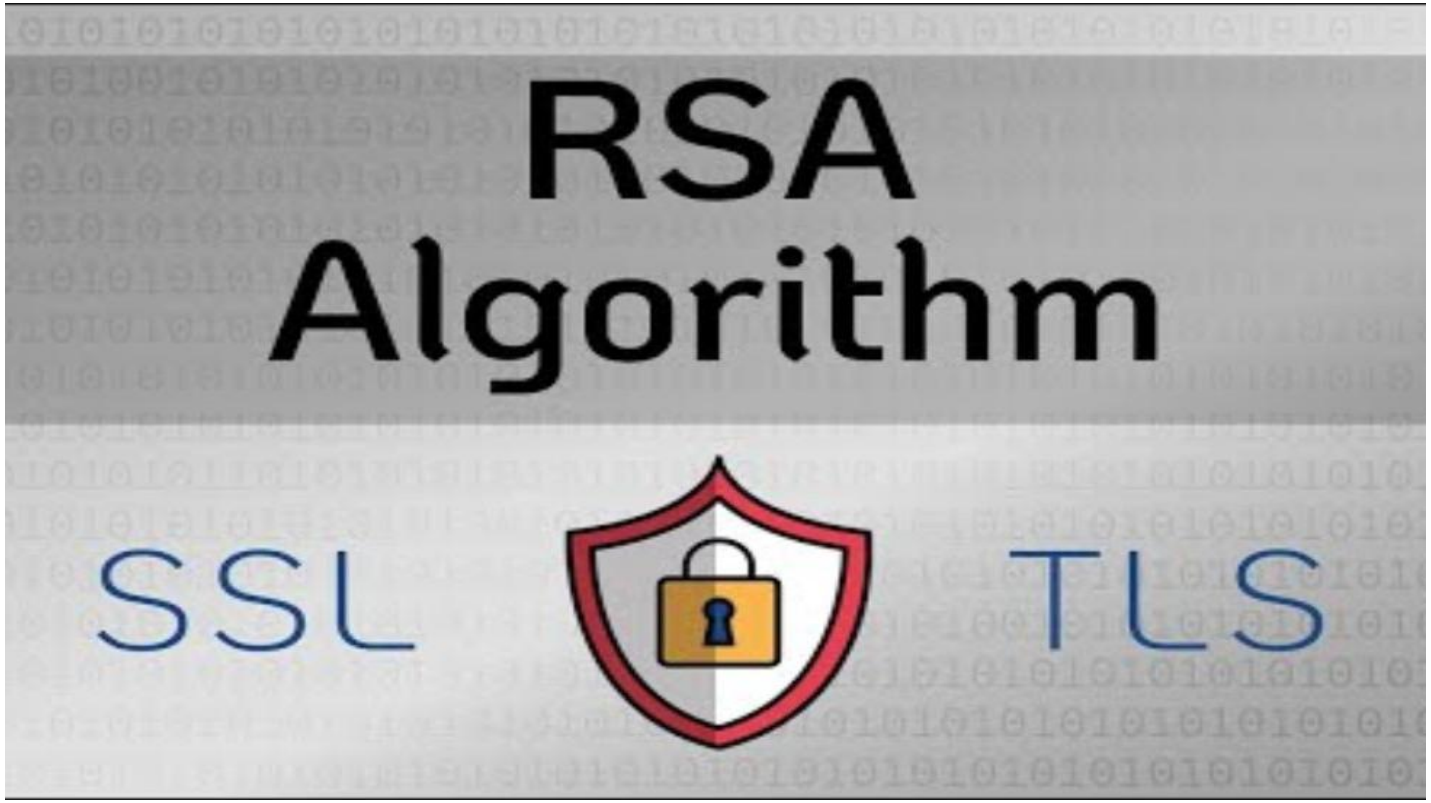
- **SubBytes:** Každý bajt sa nahradí podľa špeciálnej substitučnej tabuľky nazývanej **S-Box**. Táto operácia zavádza nelinearitu a znižuje predvídateľnosť šifrovania.
- **ShiftRows:** Každý riadok matice sa cyklicky posunie doľava o určitý počet pozícií. Prvý riadok zostáva nezmenený, druhý sa posunie o 1, tretí o 2 a štvrtý o 3 pozície. Cieľom je premiešanie bajtov medzi stĺpcami.
- **MixColumns:** V každom stĺpci matice sa aplikujú matematické operácie nad Galoisovým poľom, ktoré zabezpečia silnú **difúziu** dát – teda rozptýlenie informácie v rámci bloku. Táto operácia sa **nevykonáva v poslednom kole**.
- **AddRoundKey:** Výsledná matica sa opäť XORuje s kľúčom špecifickým pre dané kolo. Tento kľúč je súčasťou tzv. **rozšíreného kľúča**, ktorý vznikol z pôvodného tajného kľúča.

Posledné kolo:V poslednom kole sa **vynecháva operácia MixColumns** a vykonajú sa len: **SubBytes → ShiftRows → AddRoundKey. Tým sa dokončí šifrovanie jedného bloku.**

Rozšírenie kľúča (Key Expansion): proces, ktorý z pôvodného kľúča vytvorí **niekoľko subkľúčov** (jeden pre každé kolo + počiatočný). AES-128 sa z 128-bitového kľúča vytvorí **11 kľúčových blokov**.

RSA šifrovanie

- RSA (Rivest–Shamir–Adleman) je asymetrický šifrovací algoritmus, ktorý používa dvojicu kľúčov:
  - verejný kľúč na šifrovanie,
  - súkromný kľúč na dešifrovanie.
- Na rozdiel od symetrických šifier, kde obe strany musia poznať rovnaký tajný kľúč, RSA umožňuje bezpečnú komunikáciu bez predchádzajúcej výmeny tajnej informácie.
- RSA je založené na tom, že je veľmi jednoduché vynásobiť dve **veľké prvočísla**, ale extrémne ťažké ich spätne rozložiť – tento problém sa nazýva faktorizácia.
- Používa sa pri **SSL/TLS**, **e-mailoch**, **bankovníctve**, **digitálnych podpisoch**

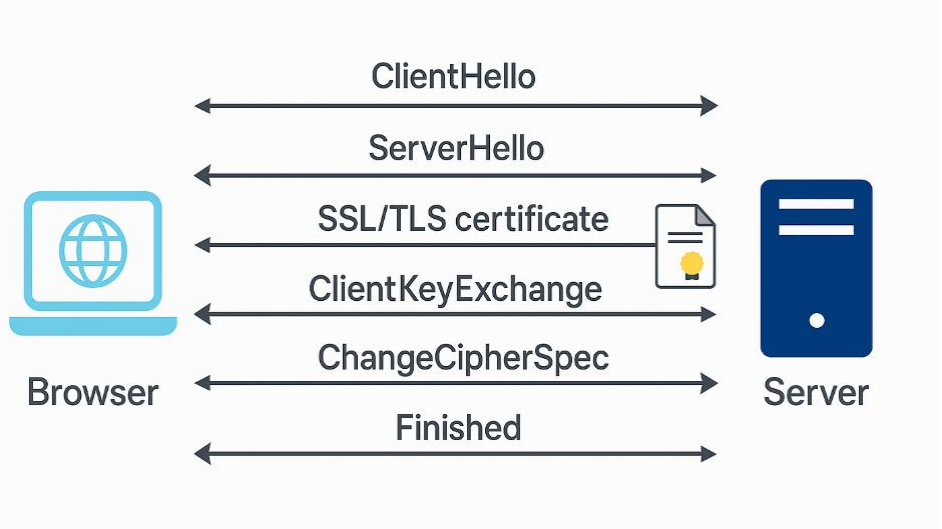


SSL resp. TLS certifikát

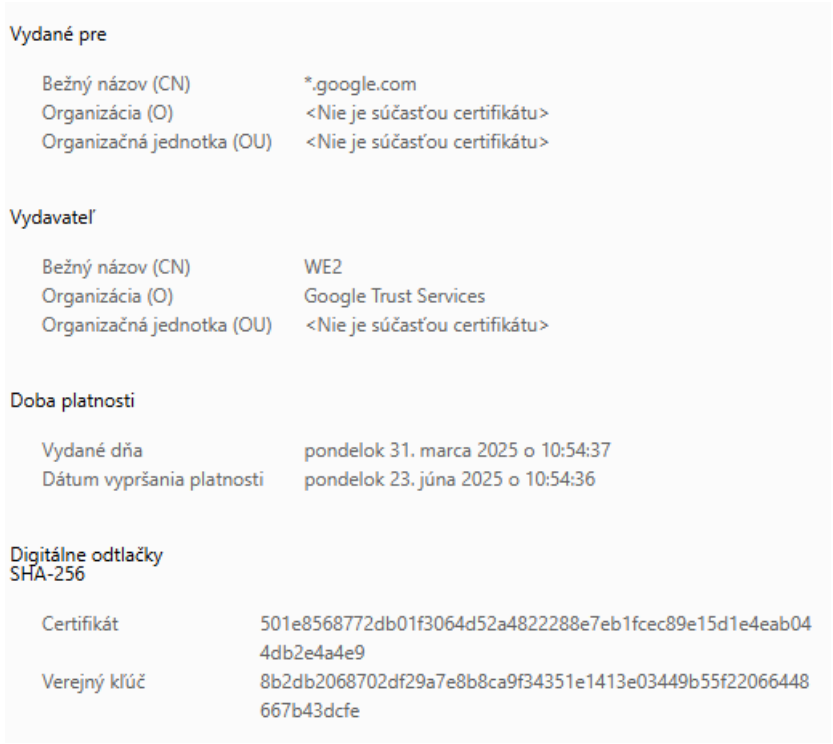
- **SSL certifikát** je **digitálny certifikát**, ktorý potvrdzuje **identitu webovej stránky** a umožňuje vytvoriť **šifrované spojenie** medzi webovým serverom a používateľom.
- **SSL** znamená **Secure Sockets Layer**, čo bol pôvodný protokol na zabezpečenú komunikáciu.
- Dnes sa používa jeho novšia verzia **TLS** (Transport Layer Security), ale ľudia stále bežne hovoria "*SSL certifikát*".
- **Overuje** totožnosť webovej stránky (že je skutočná a nefalšovaná).
- **Šifruje** komunikáciu medzi používateľom a serverom, aby údaje (napr. heslá, čísla kariet) nemohol nikto odpočúvať.
- **Zvyšuje dôveru** – web s platným SSL (TLS) certifikátom má v prehliadači ikonu zámku 🔒 a adresu začínajúcu https://.

Ako funguje SSL/TLS spojenie

1. Klient sa pripojí a požiada o bezpečné spojenie.
2. Server pošle svoj certifikát.
3. Klient overí certifikát.
4. Klient vygeneruje tajomstvo, zašifruje ho a pošle serveru.
5. Server dešifruje tajomstvo.
6. Obe strany si vytvoria rovnaké šifrovacie kľúče.
7. Celá ďalšia komunikácia je šifrovaná.



Google.com



Vydané pre

Bežný názov (CN)	*.google.com
Organizácia (O)	<Nie je súčasťou certifikátu>
Organizačná jednotka (OU)	<Nie je súčasťou certifikátu>

Vydavateľ

Bežný názov (CN)	WE2
Organizácia (O)	Google Trust Services
Organizačná jednotka (OU)	<Nie je súčasťou certifikátu>

Doba platnosti

Vydané dňa	pondelok 31. marca 2025 o 10:54:37
Dátum vypršania platnosti	pondelok 23. júna 2025 o 10:54:36

Digitálne odtlačky
SHA-256

Certifikát	501e8568772db01f3064d52a4822288e7eb1fcec89e15d1e4eab044db2e4a4e9
Verejný kľúč	8b2db2068702df29a7e8b8ca9f34351e1413e03449b55f22066448667b43dcfe

Aktivita: Overte SSL/TLS spojenie (certifikát) Vašej obľúbenej web stránky.

- Tento certifikát bol vydaný pre všetky subdomény Google, čo znamená, že platí nielen pre www.google.com, ale aj pre ďalšie služby ako mail.google.com, drive.google.com a podobne.
- Certifikát vydala spoločnosť Google Trust Services, pričom v certifikáte je ako Bežný názov (CN) uvedené WE2. To znamená, že Google si spravuje vlastnú certifikačnú autoritu a vydáva si certifikáty interne. Vďaka tomu má Google vyššiu mieru kontroly nad bezpečnosťou a správou svojich certifikátov.
- Certifikát obsahuje aj **digitálny odtlačok SHA-256**. Tento odtlačok slúži na overenie integrity certifikátu. Ak by niekto certifikát zmenil alebo sfalšoval, odtlačok by sa nezhodoval a prehliadač by upozornil na problém.
- Ďalej je uvedený aj **verejný kľúč**, ktorý sa používa pri vytváraní zabezpečeného šifrovaného spojenia.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hashovanie: digitálny podpis, ukladanie hesiel, integrita dát, blockchain, indexovanie dát db

- Hashovanie je matematická operácia, ktorá vezme vstupné údaje (napr. text, čísla, súbor) a prevedie ich na pevne dlhý reťazec znakov alebo čísel.
- Výsledok sa volá **hash** alebo **hash hodnota**.
- `import hashlib` – potrebujeme hashlib, lebo obsahuje implementácie hashovacích algoritmov (SHA-256, MD5, atď.).
- Aj keď zmeníte len jeden znak vo vstupe, výsledný hash sa úplne zmení!

Vlastnosť	Vysvetlenie
Jednosmernosť	Z hashu sa nedajú spätne vypočítať pôvodné dáta.
Deterministickosť	Rovnaký vstup vždy vytvorí rovnaký hash.
Citlivosť na zmenu	Malá zmena vstupu spôsobí úplne iný hash.
Rovnaká dĺžka výstupu	Hash má vždy rovnaký počet znakov, bez ohľadu na veľkosť vstupu.
Odolnosť voči kolíziám	Ťažké nájsť dva rôzne vstupy s rovnakým hashom. (ale nie nemožné)

Knižnice na hashovanie: hashlib

Naimportujeme knižnicu hashlib, ktorá obsahuje funkcie na hashovanie

import hashlib

Zadáme správu, ktorú chceme zahashovať

sprava = "FBI UNIZA"

Vytvoríme hash objekt pomocou funkcie sha256

Funkcia .encode() premení reťazec na bajty, pretože hashlib pracuje s bajtmi

hash_objekt = hashlib.sha256(sprava.encode())

Výsledný hash prevedieme na čitateľnú formu (hexadecimálny reťazec)

hash_hex = hash_objekt.hexdigest()

Vypíšeme výsledný hash

print(f"Hash správy: {hash_hex}")

Hash správy: af53c59af9382934bd6666acb925293b9db7a8ef28c9984f5f8eca9b823e3664

```python
# Naimportujeme knižnicu hashlib, ktorá obsahuje funkcie na hashovanie
import hashlib

# Zadáme správu, ktorú chceme zahashovať
sprava = "FBI UNIZA"

# Vytvoríme hash objekt pomocou funkcie sha256
# Funkcia .encode() premení reťazec na bajty, pretože hashlib pracuje s bajtmi
hash_objekt = hashlib.sha256(sprava.encode())

# Výsledný hash prevedieme na čitateľnú formu (hexadecimálny reťazec)
hash_hex = hash_objekt.hexdigest()

# Vypíšeme výsledný hash
print(f"Hash správy: {hash_hex}")


# Hash správy: af53c59af9382934bd6666acb925293b9db7a8ef28c9984f5f8eca9b823e3664
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

PKI - čo to je?

PKI (Public Key Infrastructure), v preklade infraštruktúra verejného kľúča, je systém technológií, pravidiel a organizácií, ktorý umožňuje bezpečnú komunikáciu v digitálnom prostredí pomocou verejných a súkromných kľúčov. PKI zabezpečuje, aby komunikácia, identifikácia a výmena dát na internete bola dôveryhodná a bezpečná.

PKI zohráva v kybernetickej bezpečnosti viacero dôležitých úloh:

- **Šifrovanie**: Zabezpečuje, aby údaje boli čitateľné iba pre správneho príjemcu.
- **Digitálne podpisy**: Overuje, že správa alebo dokument neboli pozmenené a že pochádzajú od správneho odosielateľa.
- **Overovanie identity**: Zaručuje, že webová stránka, server alebo osoba sú skutočne tým, kým tvrdia, že sú.
- **Správa kľúčov**: Zahŕňa generovanie, distribúciu, obnovu a zneplatnenie digitálnych certifikátov a kľúčov

PKI - ako funguje?

PKI je založená na niekoľkých základných prvkoch:

- **Certifikačná autorita (CA)** je dôveryhodná organizácia, ktorá vydáva digitálne certifikáty. Tieto certifikáty potvrdzujú, že určitý verejný kľúč patrí konkrétnej entite (osobe, organizácii alebo serveru).
- **Digitálny certifikát** je elektronický dokument, ktorý obsahuje verejný kľúč, identifikačné údaje vlastníka a podpis certifikačnej autority. Certifikát potvrdzuje, že verejný kľúč patrí tomu, kto tvrdí, že je jeho vlastníkom.
  - ***Kde sme sa s tým stretli?***
- **Verejný a súkromný kľúč**: Každý používateľ má dvojicu kľúčov. Verejný kľúč je verejne dostupný a slúži na šifrovanie dát alebo overovanie podpisov. Súkromný kľúč zostáva tajný a slúži na dešifrovanie dát alebo vytváranie digitálnych podpisov. **Verejný kľúč na šifrovanie → Súkromný kľúč na dešifrovanie**
- **Overenie**: Keď sa používateľ pripojí na server, jeho prehliadač overí platnosť certifikátu prostredníctvom certifikačnej autority. Ak je certifikát dôveryhodný a platný, spojenie sa považuje za bezpečné.

Príklady využitia PKI

- Pri zabezpečení webových stránok (HTTPS certifikáty),
- Pri digitálnom podpisovaní e-mailov a dokumentov,
- Pri autentifikácii používateľov vo VPN sieťach,
- Pri overovaní integrity softvérových aktualizácií.

Kľúčové pojmy spojené s PKI

- **CA (Certificate Authority)**: Organizácia, ktorá vydáva digitálne certifikáty.
- **RA (Registration Authority)**: Autorita, ktorá prijíma a overuje žiadosti o vydanie certifikátov.
- **CRL (Certificate Revocation List)**: Zoznam certifikátov, ktoré boli zneplatnené pred uplynutím ich platnosti.
- **OCSP (Online Certificate Status Protocol)**: Protokol umožňujúci online overenie platnosti certifikátu v reálnom čase.

PKI je neoddeliteľnou súčasťou bezpečnosti na internete. Umožňuje dôveryhodnú výmenu informácií, ochranu pred podvrhnutím identity a zabezpečenie komunikácie pred odpočúvaním a neoprávneným zásahom. Bez PKI by napríklad pripojenie k internetbankingu, nákup v e-shope alebo bezpečné prijímanie e-mailov nebolo možné.

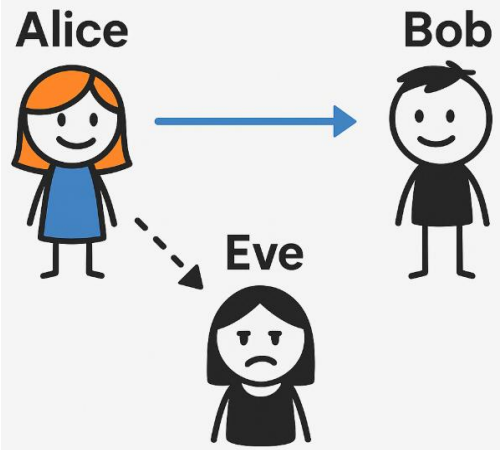
Kryptografický model (Alice, Bob, Eve)

- **Alice** – odosielateľka správy
- **Bob** – príjemca správy
- **Eve** – "*odpočúvačka*" (z anglického *eavesdropper*), teda útočníčka, ktorá sa snaží správu zachytiť

Scenár:

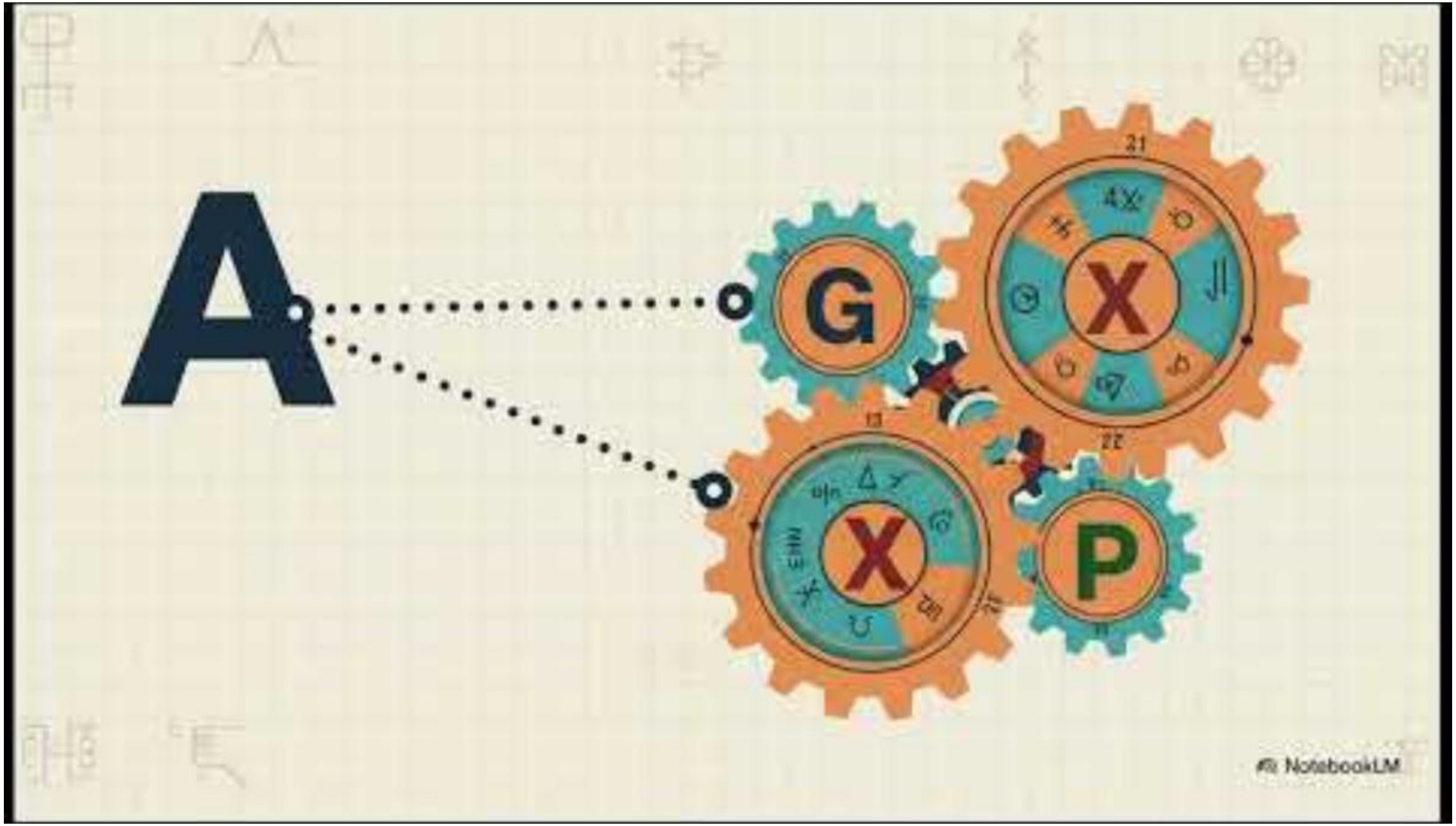
- **Alice** chce poslať správu **Bobovi**.
- Nechce, aby túto správu videl niekto iný.
- Medzi nimi je však **Eve**, ktorá môže zachytiť prenos a pokúsiť sa získať obsah správy.
- Úlohou šifrovania je **zabezpečiť**, že aj keď Eve zachytí šifrovaný text, **nedokáže ho prečítať bez kľúča**.

- **Symetrická šifra**: Alice a Bob musia **vopred zdieľať tajný kľúč**. Eve sa ho pokúša získať.
- **Asymetrická šifra**: Alice použije **verejný kľúč Boba** na šifrovanie. Len Bob má **súkromný kľúč** na dešifrovanie.
- **Digitálny podpis**: Bob overuje, že správu naozaj poslala Alice, pomocou **verejného kľúča Alice**.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zhrnutie https://youtu.be/ARJU8pxCFqU



Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Ochrana dát a súkromia

Základy kryptografie (Blok VII)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti vo verejnej správe

Ing. Ladislav Mariš, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

ladislav.maris@uniza.sk