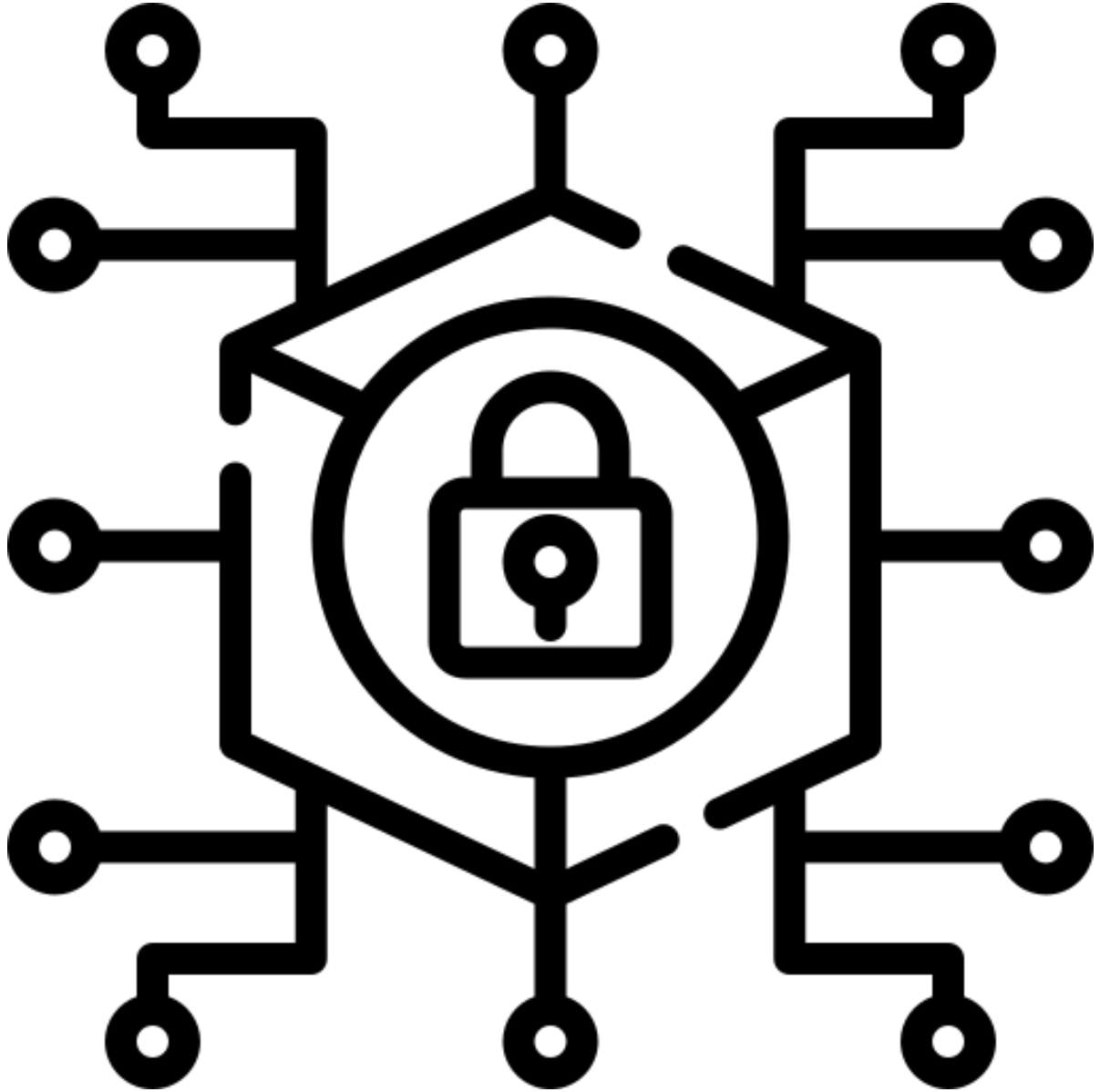
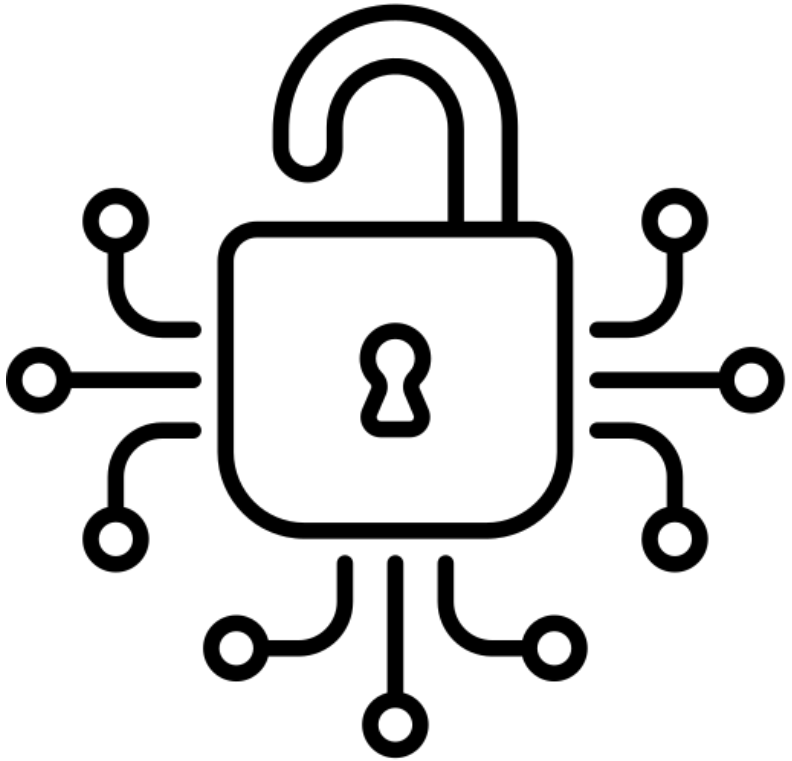
Kryptografie, Kryptoanalýza a Steganografie



Co je to kryptografie?

- Vědní disciplína, která ztělesňuje zásady, prostředky a metody pro ochranu určených informací.
- Cíl
  - Zajistit důvěrnost, integritu, autenticitu a nezpochybnitelnost dat
- Historie
  - Od starověkých šifer po moderní kryptografii

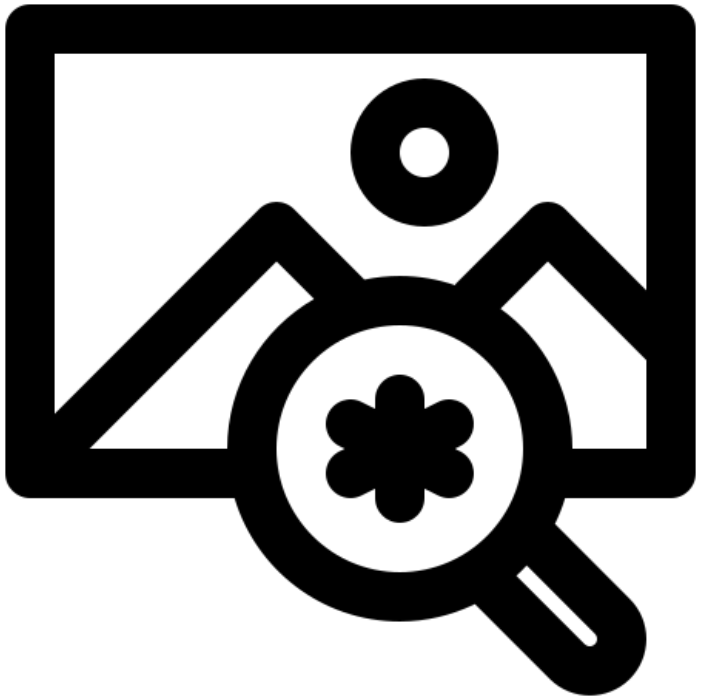


Co je to kryptoanalýza?

- Vědní disciplína, která zkoumá zásady, prostředky a metody vedoucí k získání určených informací, chráněných kryptografickými metodami, neoprávněnou stranou
- Cíl
  - Ověřit bezpečnost kryptografických systémů, rozluštit šifrované informace bez znalosti klíče

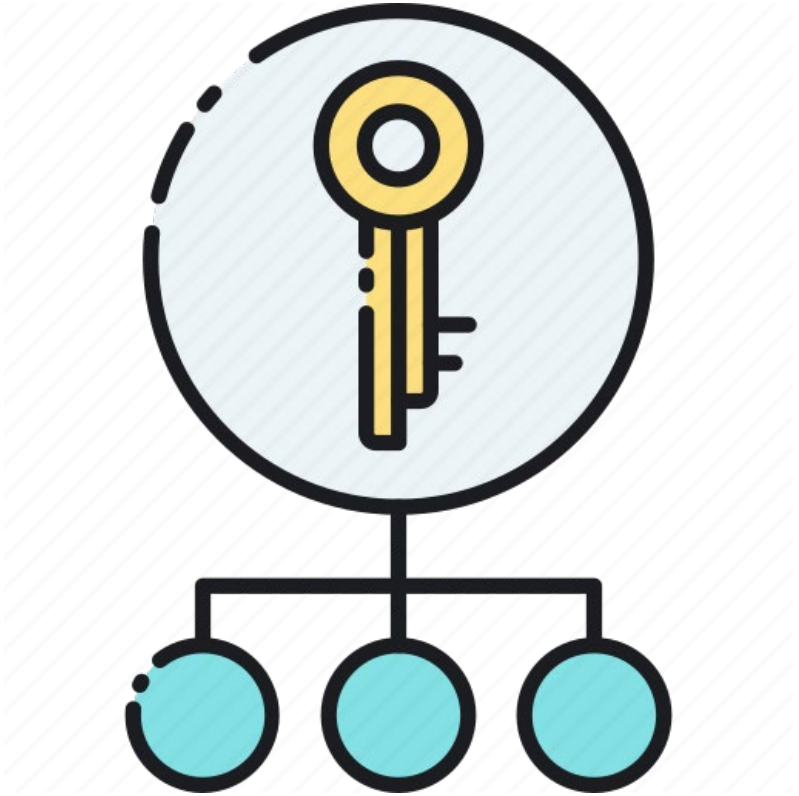
Co je to steganografie?

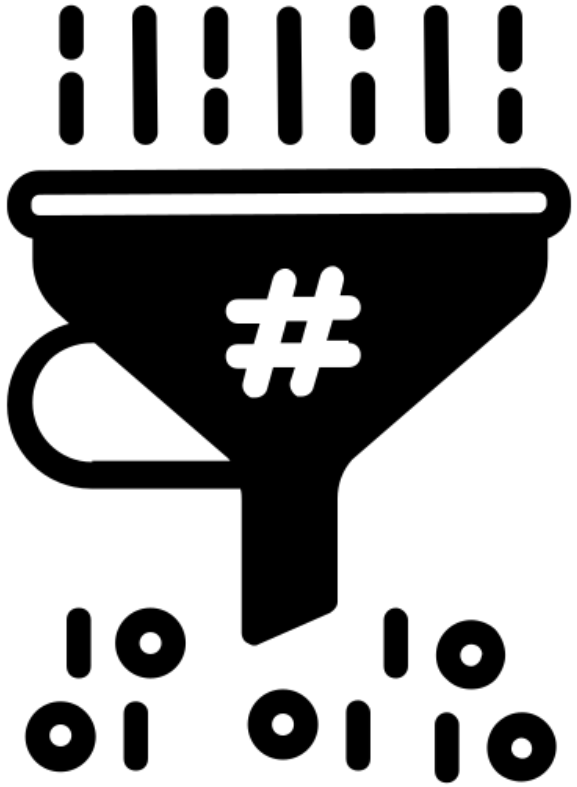
- Podobor kryptografie
- Vědní disciplína, zabývající se utajením komunikace prostřednictvím ukrytí zprávy
- Zpráva je ukryta tak, aby si pozorovatel neuvědomil, že komunikace vůbec probíhá
- Cíl
  - Umožnit přenos informací tak, aby přítomnost šifrované zprávy nebyla detekovatelná
- Příklady
  - Skryté zprávy v digitálních obrázcích nebo audio souborech



Šifry symetrické a asymetrické

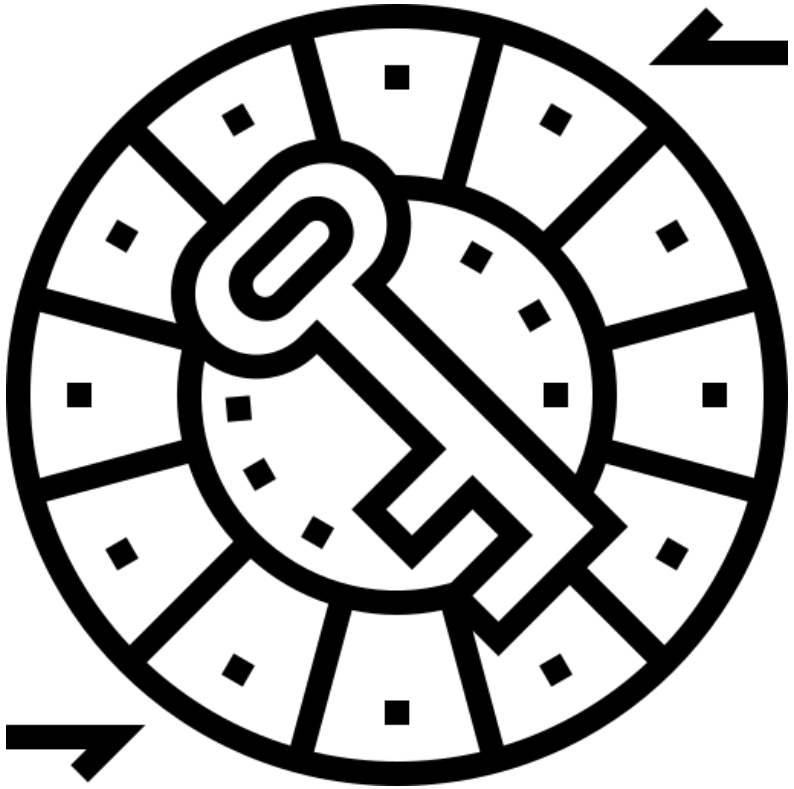
- Symetrické šifry
  - Jednoduchý a rychlý způsob šifrování.
  - Používá jeden klíč pro šifrování i dešifrování zpráv.
  - Efektivní pro šifrování velkých objemů dat.
  - AES (Advanced Ecryption Standard)
- Asymetrické šifry
  - Používá dva klíče: veřejný klíč pro šifrování a soukromý klíč pro dešifrování.
  - Umožňuje bezpečnou komunikaci bez předchozího sdílení klíčů.
  - Vhodné pro digitální podpisy a zabezpečení online transakcí.
  - Méně efektivní pro šifrování velkých objemů dat kvůli složitosti výpočtů.
  - RSA (Rivest – Shamir – Adleman)





Hashovací funkce

- Převádí vstupní data na výstup pevné délky, „otisk“ dat
- Vlastnosti
  - Odolnost vůči kolizím, skrytí originálu, rychlá výpočetní efektivita
- Použití
  - Ověření integrity dat
  - Ukládání hesel

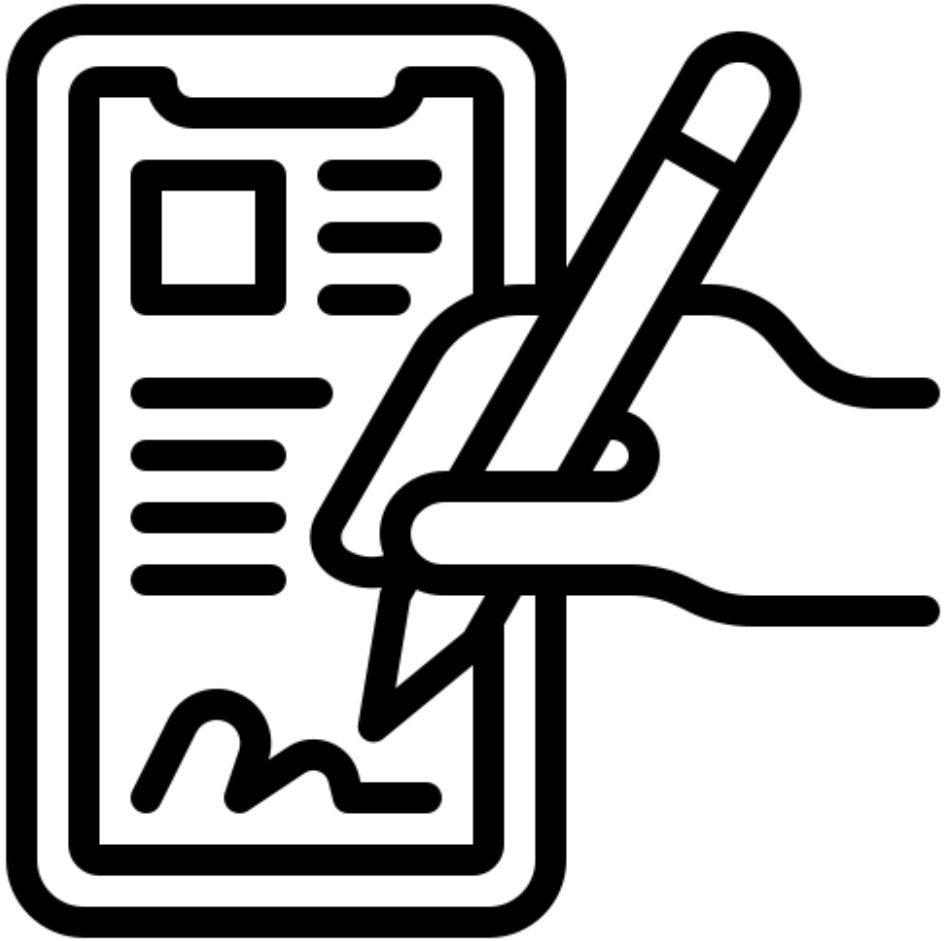


Šifry substituční a transpoziční

- Substituční šifry
  - Nahrazují jednotlivé znaky nebo skupiny znaků jinými
  - Též záměnné šifry
  - Mohou být jak symetrické tak asymetrické
  - Naprostá většina v současnosti používaných šifer jsou právě záměnné šifry
  - Například Caesarova šifra
- Transpoziční šifry
  - Mění pořadí znaků v otevřeném textu
  - Zašifrovaný text je fakticky permutací znaků otevřeného textu.
  - Například Scytale

Digitální podpis

- Zobrazení, které datovému souboru pomocí kryptografických algoritmů přiřadí (vypočítá) jiný datový soubor.
- Digitální podpis se dá využít pro elektronický podpis, ale také pro další aktivity, jako je autentizace subjektu nebo zajištění integrity vstupního souboru.



Děkuji za pozornost

Caesarova šifra

Caesaorva šifra s posunem - Původně šifra, v níž je jedno písmeno nahrazeno jiným o tři pozice dále v abecedě (A se nahradí D, B se nahradí E, C se nahradí F a tak dále). V obecnějším slova smyslu se jedná o šifru jednoduché záměny, v níž je klíč pro zašifrování cyklickým posunem abecedy o N pozic. Klasická Caesarova šifra má posun N = 3

Zašifrování s posunem n

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

Dešifrování s posunem n

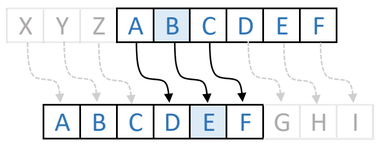
$$D_n(x) = (x - n) \bmod 26$$

Příklad zašifrování slova HELLO s posunem 3

HELLO
H → K

E → H
L → O
L → O
O → R

KHOOR



RSA algoritmus

RSA algoritmus je jedna z nejznámějších metod pro šifrování a digitální podpisy v oblasti kryptografie. Byl pojmenován po svých vynálezcích, Ronu Rivestovi, Adi Shamirovi a Leonardu Adlemanovi, kteří tento algoritmus vytvořili v roce 1977.
Jedná se o asymetrický šifrovací algoritmus což znamená, že používá dva klíče: veřejný a soukromý. Veřejný klíč může být sdílen s kýmkoliv, zatímco soukromý klíč musí zůstat tajný a je znáý pouze majiteli klíče.
Kryptosystém RSA používá jednosměrnou funkci.

Klíč se vytvoří tím, že se vynásobí dvě velká prvočísla "p" a "q" - $p * q = N$

Tato dvě čísla jsou známá pouze majiteli a ten si je nechává pro sebe. Jejich součin "N" je součástí veřejného klíče. Je tzv. modul, který spolu s číslem, kterému budeme říkat "e", tvoří veřejný klíč

V počítačovém systému se text obvykle kóduje jako ASCII nebo nějaká jiná forma binárního kódu. Už od začátku je tedy text v podstatě číslo. Označíme ho jako číslo Z a zašifrovaný text jako číslo C.

Jednosměrná funkce, kteoru použijeme, bude vypadat takto:

$$C = Z\mathrm{e}(\mathrm{mod}\, N)$$

Majitel si jako "p" vybere prvočíslo 17 a jako "q" 11; obě tato čísla drží v tajnosti. Zveřejní však veřejný klíč N, což je 17 * 11 = 187, a také číslo e - řekněme 7. Řekněme, že někdo bude chtít majiteli poslat zprávu "A". A - 65 v ASCII.
Poté svou zprávu zašifruje:

$$C = 657(\mathrm{mod}\, 187) = 142$$

Aby majitel zprávu dešifroval, musí najít svůj dešifrovací klíč pomocí následujícího vzorce:

$$d = (1/e)\,\mathrm{mod}\big((p-1)*(q-1)\big)$$

Takže:

$$d = (1/7)\,\mathrm{mod}(16*10)$$

$$d = (1/7)(\mathrm{mod}\, 160) = 23$$

Aby majitel dešifroval jednoduchou zprávu, použije tento vzorec:

$$\mathrm{Z} = C\,\mathrm{d}(\mathrm{mod}\, 187)$$

$$\mathrm{Z} = 14223(\mathrm{mod}\, 187)$$

$$\mathrm{Z} = 65, \textit{což je A v ASCII}$$

Vigènerova šifra

Vigènerova šifra - Historická polyalfabetická šifra používající periodicky krátké heslo. Zašifrování se provádí sečtením hodnoty znaku otevřeného textu (OT) se znakem hesla (H) modulo 26. Výsledkem je znak šifrového textu (ŠT)
Heslo je kratší než OT a používá se periodicky stále znovu a znovu. Symbolicky: ŠT = (OT + H) mod 26, A = 0, B = 1, …, Z=25.
Dešifrování se provádí dle vzorce: OT = (ŠT - H) mod 26

K šiforvání se využívá Vigènerův čtverec, který používá 26 cyklciky posunutých abeced.

	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

Šifra je rozložena na takzvaném "Vigènerově čtverci". Nahoře jsou napsaná písmena abecedy otevřeného textu.
Pod nimi se abeceda opakuje. Další řádky jsou postupně s cyklickým posunem o jedna. V prvním sloupci jsou písmena hesla.

Pro zašifrování zprávy Vigènerovým čtvercem potřeujete klíčové slovo (heslo) - řekněme MODRA.
Heslo je většinou kratší než otevřený text a je tedy v heslové posloupnosti (klíči) periodicky znovu používáno.

Otevřený text	p o s l e t e k a n o n n a k o p e c
Heslová posloupnost	M O D R A M O D R A M O D R A M O D R
Zašifrovaný text	B C V C E F S N R N A B Q R K A D H T

K dešifrování zprávy potřebuje příjemce znát klíčové slovo - potom stačí celý proces obrátit

Hillova šifra

Hillova šifra je klaciský šifrovací systém založený na lineární algebře, který byl vynalezen Lesterem S. Hillem v roce 1929.
Tento systém používá matematické principy pro transofrmaci textu na základě maticových operací, což představuje zajímavý odchod od tradičních šifrovacích metod založených na substituci a transpozici
Klíčovým prvkem Hillovy šifry je použití šifrovací matice, která slouží jako šifrovací klíč. Tato matice musí být invertibilní v moudlární aritmetice (obvykle se používá modul odpovídající počtu písmen v abecedě, například 26 pro anglickou abecedu), aby bylo možné zprávu dešifrovat

Šifrace:

Pro zašifrování zprávy "ACT" (n=3). Klíč je "GYBNQKURP" což se jako nxn matice napíše takto:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Zpráva "ACT" jako vektor

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Zašifrovaný vektor bude vypadat takto:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} (\mathrm{mod}\ 26)$$

Což odpovídá šifrovanému textu "POH"

Dešifrace:

Pro dešifrování zprávy, se zašifrovaný text vrátí do podoby vektoru, a potom se vynásobí převrácenou maticí klíčové matice (IFKVIVVMI v písmenech)

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 70 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 27 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

Pro předešlý zašifrovaný text (POH):

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} (\mathrm{mod}\ 26)$$

Dešifrovaný text odpovídá původnímu slovu "ACT"

Vernamova šifra

Vernamova šifra, známá také jako jednorázový blok je typ šifrování, který byl vynalezen a patentován Gilbertem Vernamem v roce 1917. Tato šifra je v kryptografii známá jako jedna z mála dokonale bezpečných šifrovacích systémů, pokud je správně použita
Vernamova šifra funguje na jednoduchém principu: každý bit nebo písmeno prostého textu(plain textu) je zašifrováno pomocí binární operace XOR s přesně jedním bitem nebo písmenem tajného klíče, který je náhodně generován a má stejnou délku jako prostý text.
Klíč se používá pouze jednou, a proto se nazývá "jednorázový blok"

Šifrace:

Prostý text: O A K
Klíč: S O N

Nejdříve se vypočítá pozice v abecedě, která se potom převede do binární verze:
O ==> 14 = 0 1 1 1 0
S ==> 18 = 1 0 0 1 0

Potom se využije binární operace XOR, která funguje tak, že porovná vstupní bity, a pokud jsou stejné vrátí 0 a pokud jsou jiné vrátí 1:

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

XOR

bitový XOR výsledek:
1 1 1 0 0 = 28

Pokud je XOR výsledek větší než 26, odečtě se číslo 26 od výsledného čísla:

28-26 = 2 ==> C
Zašifrovaný text: C

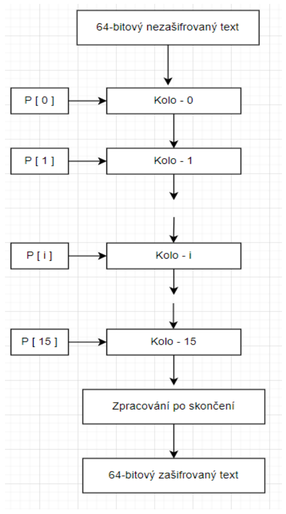
Celý zašifrovaný text:
Prostý text: O A K ==> 14 00 10
Klíč: S O N ==> 18 14 13
ZT-čísla: 02 14 07
ZT: C O H

Pro dešifraci se využije otočený postup

Blowfish

Blowfish je šifrovací algoritmus navržený Brucem Schneierem v roce 1993 jako alternativa k starším šifrovacím algoritmům, jako je DES (Data Encryption Standard). Blowfish je známý svou rychlostí a efektivitou, zejména v systémech, kde jsou zdroje omezené.
Blowfish je symetrická bloková šifra, což znamená, že šifruje data ve fixních velikostech bloků (u Blowfish je to 64 bitů) a používá stejný klíč pro šifrování a dešifrování. Má variabilní délku klíče od 32 do 448 bitů, což poskytuje dobrý kompromis mezi bezpečností a výkonností
Je značně rychlejší než DES a má dobrý šifrovací výkon. Do dnes nebyla nalezena žádná účinna technika kryptoanalýzy, která by tento algoritmus dokázala spolehlivě prolomit

Šifrace:



Kde P odpovídá seznamu subklíčů, pomocí kterých probíhá šifrace