Historické šifry crypto

Challenge status: **Available**
Challenge flags: **5**

Odkryjte tajemství historického šifrování. Od Caesarovy šifry, Vigenèrovy šifry, až k dokonale bezpečnému One-time padu. Seznámíte se s termíny substituce a transpozice a pro složitější případy si ukážeme online nástroje, které Vám v prolamování šifer pomůžou.

Theory | Flags | Handbook | Solves

Co vlastně kryptografie je a k čemu složí?

Kryptografie má své kořeny až v dávných dobách, kdy lidé potřebovali posílat tajné zprávy a nechtěli, aby je někdo jiný četl. Mohlo se jednat o zamilovaný dopis nebo třeba o plán dalšího útoku při válce. Dnes je kryptografie důležitější než kdy předtím. S rostoucím významem internetu a digitálních technologií se stále více informací přenáší přes sítě a je třeba je chránit před digitálními zloději. Než se ale vrhneme na to, jak se počítá RSA a ostatní moderní kryptografické algoritmy, tak je potřeba vrátit se na začátek.

Caesarova šifra

Píše se rok 100 před naším letopočtem a Julius Caesar potřeboval poslat generálovi tajnou zprávu. Julius Caesar si byl vědom toho, že pokud bude zpráva zachycena nepřítelem, může to znamenat ztrátu bitvy a možná i celé války. Proto si Caesar připravil speciální šifru, kterou mohl použít k šifrování zpráv a ta je dnes známa jako Caesarova šifra.

Jak funguje?

Princip této šifry je na dnešní poměry velice jednoduchý. Jedná se o substituční šifru, která nahrazovala každé písmeno v abecedě o určitý počet pozic dopředu nebo dozadu. Caesar si zvolil posun o 3 pozice dopředu, což znamenalo, že písmeno A bylo nahrazeno písmenem D, písmeno B bylo nahrazeno písmenem E a tak dále. Posun však může být o libovolný počet písmen. Pro dešifrování stačí posunout písmena na druhou stranu.

Příklad Caesarovy šifry:

- Původní text: `ahoj tady caesar`
- Posun o +3 písmena: `dkrm wdgb fdhvdu` (zašifrovaný text)
- Posun o -3 písmena: `ahoj tady caesar` (odšifrovaný text)

Zkuste si to klidně sami. Zašifrujte si krátkou zprávu a prohoďte si ji se sousedem v lavici. (Nezapomeňte mu říci kolik je posun) Pro Caesarovu šifru existuje mnoho nástrojů online ale vzhledem k tomu, že se jedná o vskutku jednoduchou šifru, tak si to můžete zkusit čistě na papíře.

> *Existuje šifra identická Ceasarově, ale jmenuje se ROT13. Jediný rozdíl je, že místo standardního posunu o 3 je posun o 13. Funguje však úplně identicky.*

Vigenèrova šifra

Jedná se o polyalfabetickou substituční šifru. Funguje velmi podobně jako Caesarova šifra, je jen o trochu složitější. Místo toho, aby posun byl pouze jedno číslo a všechna písmena se posunula stejně, tak je posun udáván klíčem. První písmeno je posunuto o hodnotu prvního písmena klíče, druhé písmeno je posunuto o hodnotu druhého písmena klíče atd... Pokud je klíč kratší než původní zpráva, tak klíč opakujte stále dokola.

Tabulkový způsob

Nejnázornější je způsob s tabulkou, kde si v horním řádku vybíráte písmena původní zprávy a v levém sloupci vybíráte písmena klíče. Tam kde se protnou je vaše zašifrované písmeno zprávy.

		původní zpráva																								
		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
k	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
l	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
í	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
č	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

Názorně si ukážeme:

- Původní text: `hello`
- Klíč: `key`

V horním řádku vyberte písmeno `H`, v levém sloupci vyberte písmeno `K` a protnou se na písmeně `R`. V horním řádku vyberte písmeno `E`, v levém sloupci vyberte písmeno `E` a protnou se na písmeně `I`. V horním řádku vyberte písmeno `L`, v levém sloupci vyberte písmeno `Y` a protnou se na písmeně `J`. V horním řádku vyberte písmeno `L`, v levém sloupci vyberte písmeno `K` a protnou se na písmeně `V`. V horním řádku vyberte písmeno `O`, v levém sloupci vyberte písmeno `E` a protnou se na písmeně `S`.

Zašifrovaný text je `RIJVS`

Odšifrování zprávy:

Zprávu odšifrujete tak, že si v levém sloupci najdete písmeno klíče a uvnitř tabulky na stejném řádku najdete písmeno zašifrovaného textu. Výsledné odšifrované písmeno bude v horním řádku.

V levém sloupci vyberte písmeno `K` a v tomto řádku najděte písmeno `R`. V horním řádku tato pozice odpovídá písmenu `H`. V levém sloupci vyberte písmeno `E` a v tomto řádku najděte písmeno `I`. V horním řádku tato pozice odpovídá písmenu `E`. V levém sloupci vyberte písmeno `Y` a v tomto řádku najděte písmeno `J`. V horním řádku tato pozice odpovídá písmenu `L`. V levém sloupci vyberte písmeno `K` a v tomto řádku najděte písmeno `V`. V horním řádku tato pozice odpovídá písmenu `L`. V levém sloupci vyberte písmeno `E` a v tomto řádku najděte písmeno `S`. V horním řádku tato pozice odpovídá písmenu `O`.

Matematický způsob

Pokud máte raději vzorce než hledání písmenek v tabulce, tak tento způsob bude pro Vás vhodnější.

Každé písmeno si převedeme na číslo udávající jeho pozici v abecedě počínaje nulou (ABCDEFGHIJKLMNOPQRSTUVWXYZ). Například A = 0, Z = 25. Vigenèrova šifra používá pro šifrování a odšifrování klíč, kde každé písmeno klíče udává posun jednoho písmena původního textu. Nejjednodušší to bude vysvětlit na příkladu:

- Původní text: `hello`
- Klíč: `key`

Nejprve převeďte zprávu a klíč na čísla

- Původní text: `7 4 11 11 14`
- Klíč: `10 4 24`

Každé číslo původního textu sečtěte s číslem klíče a na výsledek aplikujte modulo 26. Pokud je klíč kratší než původní zpráva, tak klíč opakujte.

```
(7+10)  % 26 = 17
(4+4)   % 26 = 8
(11+24) % 26 = 9
(11+10) % 26 = 21
(14+4)  % 26 = 18
```

Po převedení čísel opět na písmena je zašifrovaný text: `rijvs`.

Pro odšifrování následujte podobný postup akorát od zašifrovaného textu odečítejte klíč.

```
(17-10) % 26 = 7
(8-4)   % 26 = 4
(9-24)  % 26 = 11
(21-10) % 26 = 11
(18-4)  % 26 = 14
```

Jak můžete vidět, tak hodnoty po odšifrování jsou stejné jako hodnoty před zašifrováním. Po převedení čísel do textu vznikne původní slovo `hello`.

> *Pokud potřebujete prolomit šifru, ale neznáte její klíč můžete použít buďto dCode nebo Guballa.*

One-time pad

Šifra přezdívaná one-time pad (česky Vernamova šifra) používala stejného principu jako Vigenèrova šifra, ale měla následující podmínky:

- Klíč musí být vždy alespoň tak dlouhý, jako zpráva.
- Klíč musí být kompletně náhodný. Takže žádné pseudo náhodné generátory čísel, ale čistě hardwarová náhodnost.
- Klíč musí být použit maximálně jednou. Z toho plyne jméno one-time pad.
- Klíč musí být udržován v tajnosti.

Pokud dodržíte tyto podmínky, tak je šifra v principu neprolomitelná.

> *Klíče byly při válce distribuovány jako tabulky na papíře, ale občas byla pro tisk používaná i silně hořlavá nitrocelulóza.*

Scytale

Jedná se o úplně nejstarší šifru zaznamenanou v lidské historii. Datuje se až do roku 700 před naším letopočtem. Byla používaná v Řecku pro válečnou komunikaci.

Jde o transpoziční šifru, kde byl pásek papyru či pergamenu namotán na válec o předem dohodnutém rozměru a ve směru hlavní osy válce na něj byl psán text.

Následující obrázek demonstruje, jak vypadá pásek s textem namotán na válci:

```
      |   |   |   |   |   |   |
      | P | O | M | O | Z |   |
    __| M | I | J | S | E |__ |
   |  | M | P | O | D | P |
   |  | A | L | B | O | U |
   |  |   |   |   |   |   |
```

Po rozmotání je text na pásku nečitelný: `PMMAOIPLMJOBOSDOZEPU`.

Zjednodušeně by se ale tato šifra dala popsat jako vybírání x-tého písmena. A to, kolik písmen překročíte udává průměr válce. Například v našem případě se přeskakují vždy 3 písmena. Pokaždé co dojdete na konec pásku, tak začnete o jednom písmenu dál:

PMMA**O**IPL**M**JOB**O**SDO**Z**EPU (POMOZ) P**M**MAO**I**PLM**J**OBO**S**DOZ**E**PU (MIJSE) PM**M**AOI**P**LMJ**O**BOS**D**OZE**P**U (MPODP)
PMM**A**OIP**L**MJO**B**OSD**O**ZEP**U** (ALBOU)

Substituce vs transpozice

Asi jste si všimli, že jsem již několikrát použil slůvko substituce nebo transpozice. Některé šifry jsou substituční, některé transpoziční a některé dokonce obojí najednou. Tak si v tom pojďme udělat pořádek.

Substituční šifrou se rozumí šifra, která nahrazuje (substituuje) písmena za jiná písmena, ale nemění přitom jejich pořadí. Takže když se nad tím zamyslíte, tak Caesarova šifra je ukázková substituční šifra.

Na druhou stranu transpoziční šifra je taková, která přehazuje pořadí písmen. Zde je možností mnoho, ale když si vezmete jako příklad Scytale, tak to je opět ukázková transpoziční šifra.

Online nástroje

U delších textů nebo úloh, kde jsou šifry komplikovanější Vám přijdou vhod online nástroje. Jak budete v kryptografii postupovat dále uvidíte, jak užitečné doopravdy jsou. Do začátku si ale řekneme o dvou nejznámějších. dCode a CyberChef

dCode

Umí opravdu hodně šifer i včetně těch méně známých. Hlavní výhodou je, že u hodně šifer umí bruteforcnout klíč. Například u Caesarovi šifry je maximálně 26 možností zašifrování, takže pokud se podíváte na všech 26, tak uvidíte, co je text a co je pouze změť písmen. Toto ale umí i sám. Porovnává výsledky se slovy ze slovníku, takže díky tomu umí prolomit i kratší klíče u Vigenèrovy šifry a mnoha dalších. V levém horním rohu je search bar, který slouží pro vyhledávání druhů šifer.

Bohužel jeho hlavní limitací je, že dokáže pracovat pouze s jednou šifrou najednou. Nijak se nedají řetězit výstupy do vstupů a obecně mi přijde jeho rozhraní lehce zastaralé.

CyberChef

Na druhou stanu CyberChef vám vždy uvaří co potřebujete. Hlavně si určitě oblíbíte jeho modul `Magic`, který se pokusí automaticky prolomit zašifrovaný text.

V levém horním rohu můžete vyhledávat, dvojklikem modul přidáte. Tím se přidá doprostřed okna a pokud byste chtěli modul odstranit, tak na něj opět dvakrát klikněte. Okna input a output jsou myslím dostatečně jasná.

> *V nástroji CyberChef se Caesarova šifra jmenuje ROT13.*

Task 01

Ave Caesar

Následující text byl zašifrován Caesarovou šifrou s posunem +5 `mfcflts{Fa3_Hf3x4w_14K45ziZc}`.

> *Použijte standardní Caesarovu šifru, kde s posouvají pouze písmena.*

Task 02

Ave Caesar 2

Následující text byl zašifrován Caesarovou šifrou: `atqtzhg{V43lTk_1l_G0m_L3vnkx_hYo28L13}`. Rozšifrujte text, aniž byste znali původní posun.

Task 03

Vigenèr

Odšifrujte text `zezuxsf{F3vnv4_xz4R_eU3j4V_Ab48q1m}`. Byl vytvořen Vigenèrovou šifrou s klíčem `secure`.

Task 04

Vigenèr 2

Prolomte klíč a odšifrujte následující text.

> *Text byl vytvořen Vigenèrovou šifrou a je v angličtině.*

```
Oirzntke ndpwxr tn a bxtsjd dy eyxrnittig pepsvbtmin oemm bj psxgg l negbed jf xgtpmwdoey Xatlac xieaecn, bpleo
```

Jako odpověď zapište první slovo z odšifrovaného textu, "podtržítko" a klíč v následujícím formátu `haxagon{slovo_klíč}`. (Vše malými písmeny).

> *Například kdyby první slovo bylo `Ahoj` a klíč k odšifrování byl `key`, tak odpověď bude `haxagon{ahoj_key}`.*

Task 05

Zachycená komunikace

Představte si, že jste ve válce, a právě jeden váš špión zachytil pásek pergamenu s podivným textem. Pravděpodobně se jedná o komunikaci nepřítele. Na pásku je napsáno:

```
A
A
A
O
T
C
T
O
T
K
N
N
```

Odšifrujte ho a jako odpověď napište text malými písmeny a bez mezer dovnitř závorek: `haxagon{odsifrovanytex}`.