Průvodce šiframi - jednoduché šifry

Vložil/a Wasekk [1], 3 Červenec, 2006 - 11:49

- Encryption [2]
- Security [3]

Dostali jste se někdy k šifrované zprávě? Nevíte jak ji rozluštit? Nebo naopak potřebujete zprávu zašifrovat? Dobrá, tak tedy vám poradím. Jsem doslova(neberte mě vážně) odborník na slovo vzatý.

Nejprve všechny upozorňuji, že se nebude jednat o nějaké moc složité šifry. Předpokládám, že dojde i na další díly, kde se dostanu k modernějším, ale to vůbec není jisté. A pro informaci: nehodlám zde psát o hashích a jejich ''decryptování''. A nyní již jdeme na ty šifry.

1) Caesarova šifra

Římský císař nikdy nepatřil k důvěřivým lidem. Jeho tajné, milostné i státnické, dopisy Kleopatře byly zašifrovány jednoduchým způsobem – posunutím abecedy (monoalfabatická substituce). Něco jako:
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
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
Tento systém má jednu 'drobnou' nevýhodu. Pokud se dostane do rukou někomu, kdo má dostatečné znalosti, může být prolomena. Krom toho v době počítačů a internetu ji prostě přepíšete do počítače, najdete stránku která provádí takzvanou Ceasar bruteforce. A když nenajdete program pro toto? Co třeba zkusit frekvenční analýzu? Aha, co to je. Frekvenční analýza je možnost dešifrace tím, že znáte vlastnosti jazyka. Třeba v češtině se často opakuje ve slovech E a samostatně nejčastěji A. Pokud ani to nepomůže, nezoufejte. Máte jen 25 možností (písmen v abecedě je 26).

2) Číslicová abeceda

Jestli se vám vybaví binární kód, tak jste vedle. Číslicová abeceda se využívá jako základ pro další 'čachry a machry' a není vůbec těžká. To je její slabina – bez dalšího zpacování není bezpečná. A jak vypadá?
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
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Snadné co?

3) Polyalfabetická substituce – Leon Battista Alberti

To jméno v názvu není jen tak, tuto šifru totiž vynalezl Leon Battista Alberti. Není na ní nic sloožitého, jsou to vlastně dvě Caesarovy šifry u sebe. Dohodnete se na posunutí obou dvou a můžete vesele šifrovat. Střídáte jednu s druhou. Jde samozřejmě i více abeced, ale to snad nemusím říkat, ne? Ukázka nebude, jen zkuste rozšifrovat toto: ENCQF!

4) Vigenérova tabulka

Pokud se vám zalíbila možnost minulá (znáte odpověď? Ne? Zněla DOBŘE), jistě oceníte i tento čtverec 26×26 znaků. Jedná se o množství abeced, každá začíná jiným písmenem, kdy si zvolíte klíčové slovo (key) a to opakujete po celou délku zprávy. Příklad (Vynechám diakritiku):
LIONLIO NLIO NL IONL IONLION LIONL IONL IO NLIO
BRITOVÉ JDOU DO BOJE, NEZBÝVÁ MNOHO ČASU NA ÚTĚK.

QJUGDNQ WSGG QD TAWT, FQMQQHN BFAUD UAFJ FA HIWW.
A jak postupují luštitelé? Hledají podpis (pokud znají vaše jméno a souhlasí počet písmen, je to ono). Hledají často se opakující písmena (uprostřed slov E, samotné A, pokud máte AxE, tak je to ALE...) mají samozřejmě problém s klíčem, nadruhou stranu A znamená většinou A, takže mají práci lehčí (chyták je když v klíči O šifruje o, vznikne také A). Po sobě často následují dvojice ne;st;te...

0,1234..) Morseovka

morseova abeceda není šifra sama o sobě, ale pomůže vám, když se chcete pojistit. Hlupák, který by vše vyzradil na to nepřijde a chytrák si to nechá pro sebe... krom toho ta šifra vydrží o dvacet (se štěstím) minut déle.

5) Tabulky

Takže.. spočítejte počet písmen a zjistěte, čím je dělitelný. Potom je napište do řádků např. po pěti. Nyní vemte každý sloupec a udělejte z něj jedno „slovo“. A teď napište v předem daném pořadí všechny sloupcová 'slova'.
Ještě je jeden typ tabulek. Znáte A0, C4, F2,A2? Uděláte mřížku, nahoru napíšete písmena, doleva číslice a používáte jako souřadnice... To se ovšem dá dopátrat... Tabulku si děláte buď 5×5 nebo 5×6. v prvním případě je pro J a I stejná souřadnice.

Pro dnešek vše, loučím se. Zdar! 01 08 15 10!

URL článku:
https://security-portal.cz/clanky/pr%C5%AFvodce-%C5%A1iframi-jednoduch%C3%A9-%C5%A1ifry

Odkazy:
[1] https://security-portal.cz/users/wasekk
[2] https://security-portal.cz/category/tagy/encryption
[3] https://security-portal.cz/category/tagy/security