Afinní šifra

Afinní šifra spadá mezi monoalfabetické šifry ( každý znak je nahrazen konkrétním znakem ). Rozdíl mezi Afinní a Caesarovou šifrou je ten, že kombinuje násobení a posun – kombinace lineárního šifrování.

Využívá modulární aritmetiku, což je matematický systém, ve kterém se čísla "otáčejí dokola" při dosažení určité hodnoty (modulu).

Afinní šifra je v podstatě **lineární transformace** v rámci modulární aritmetiky:

1. **Násobení klíčem a**: To způsobí **roztáhnutí a přeházení pozic znaků** v abecedě.
2. **Přičítání klíče b**: To způsobí **posunutí znaků** o konkrétní hodnotu.

a\*ot +b mod 26

Klíč a musí být nesoudělný s délkou abecedy, aby bylo možné provést dešifrování.

Abychom původní zprávu dostali zpět, musíme obrátit lineární transformaci:

D(y) = a−1⋅(y−b) mod

* Odečteme b (posun).
* Vynásobíme výsledkem inverzní hodnotou a−1.

Playfair šifra

Je založena na principu substituce párových písmen ( bigramů ). Pokaždé šifruje dvojici písmen najednou. Základem playfair šifry je tabulka 5x5, která obsahuje abecedu ( písmeno J je nahrazenou písmenem I ) a mřížka je sestavena na základě klíčového slova, které určuje uspořádání mřížky.

Zpracování po dvojicích přináší do šifry větší variabilitu a **komplikuje frekvenční analýzu**, protože počet možných kombinací bigramů je větší než počet jednotlivých písmen.

Každý pár písmen je šifrován na základě **polohy písmen v mřížce**. Playfair šifra pracuje s těmito třemi základními pravidly:

1. **Stejný řádek**: Pokud jsou obě písmena v **jednom řádku** tabulky, posuneme je **doprava** (nebo na začátek řádku, pokud je písmeno na konci).
2. **Stejný sloupec**: Pokud jsou obě písmena ve **stejném sloupci** tabulky, posuneme je **dolů** (nebo na začátek sloupce, pokud je písmeno na konci).
3. **Obdélník**: Pokud tvoří písmena **vrcholy obdélníku** v tabulce, nahradíme je písmeny na opačných stranách **řádku**.

Při **přetečení řádku** (když šifrované písmeno je na konci řádku a má být posunuto doprava) Playfair šifra **„přeskočí“ na začátek stejného řádku**.

Požadavek na **8 znaků** (nebo více) zajišťuje dostatečně náhodné rozmístění písmen, což ztěžuje prolomení šifry.

ADFGX a ADFG(V)X šifra

Substituce: znamená nahrazení původních znaků zprávy jinými znaky podle předem daného pravidla. V ADFGX a ADFGVX je toto pravidlo určeno mřížkou ( 5x5 ADFGX, 6x6 ADFG(V)X ).

Po substituci přichází druhý krok – transpozice. Transpozice znamená přeskupení znaků zprávy podle určitého pravidla. U šifer ADFGX a ADFG(V)X se používá klíčové slovo k určení, jak se znaky přeskupují. Znaky se nejdříve zapíší do tabulky a poté se čtou po sloupcích a následně se řadí podle abecedního pořadí písmen v klíči.

ADFGX a ADFGVX jsou **silné** šifry pro svou dobu díky kombinaci dvou šifrovacích technik:

1. **Substituce** rozbije původní znaky na jiné symboly.
2. **Transpozice** zamíchá pořadí těchto symbolů.

Díky tomu je **příjemce schopen zprávu dešifrovat**, pokud zná **klíčové slovo** a **mřížku**.

RSA šifra

RSA algoritmus využívá **matematické vlastnosti prvočísel** a jejich násobení. Jeho bezpečnost je založena na faktu, že **násobení dvou velkých prvočísel je snadné**, ale **rozložení výsledného čísla zpět na prvočinitele (tzv. faktorizace) je extrémně obtížné**.

Tato **jednosměrná vlastnost** dělá z RSA ideální algoritmus pro šifrování:

1. **Snadné (rychlé) násobení** dvou velkých prvočísel p a q → získáme číslo n.
2. **Obtížné (pomalé)** rozložení n zpět na p a q, pokud neznáme původní prvočísla.

**Základní myšlenka:**

* **Veřejný klíč** (který obsahuje n a e) je dostupný všem.
* I když máte veřejný klíč, nedokážete "uhádnout" soukromý klíč d, protože byste museli rozložit číslo n na p a q.

Eulerova funkce udává počet kladných celých čísel menších než n, která jsou s n **nesoudělná.**

Pro RSA, kde n = p⋅q , platí jednodušší vzorec, protože p a q jsou vždy prvočísla:

FI (n) = (p−1) ⋅ (q−1)

Je zásadní pro generaci soukromého klíče d.

DSA šifra

DSA je založený na několika klíčových matematických principech.

**A. Asymetrická kryptografie**

* **Asymetrická kryptografie** používá dva klíče:
  + **Soukromý klíč** (jen ty ho znáš).
  + **Veřejný klíč** (každý ho může znát).
* Tyto klíče jsou vzájemně propojené matematickou funkcí, ale není snadné ze znalosti veřejného klíče zjistit ten soukromý.

DSA využívá **modulární aritmetiku** a tzv. **diskrétní logaritmus**, což je matematický problém, který je velmi těžké vyřešit.

**B. Diskrétní logaritmus – základ bezpečnosti**

* Diskrétní logaritmus říká: když máme rovnici y = gxmod  p, kde:
  + g je generátor (dané číslo),
  + p je velké prvočíslo,
  + x je tajné číslo (tvůj soukromý klíč),
  + y je výsledná hodnota (tvůj veřejný klíč),
* Je **snadné spočítat y, když známe g, x a p**. Ale **je extrémně obtížné zjistit x (soukromý klíč), když známe y, g a p**.
* Tento problém se nazývá **diskrétní logaritmus,** a právě jeho obtížnost zaručuje bezpečnost DSA.

**Hashování zprávy:**

* Nejprve vezmeš zprávu a vytvoříš z ní její **otisk (hash)**.
* Hashovací funkce (např. SHA-256) vezme libovolně dlouhý text a vytvoří krátký, pevně dlouhý řetězec (např. 256 bitů), který reprezentuje obsah zprávy.

**Podepsání hashe pomocí soukromého klíče:**

* Když vytvoříš hash, podepíšeš ho svým **soukromým klíčem**.
* Matematika DSA ti umožní vytvořit podpis (dvě hodnoty r a s) tak, že:
  + Podpis je **unikátní** pro daný hash zprávy a náhodné číslo k.

Příjemce (např. Bob) ověřuje podpis pomocí tvého **veřejného klíče**:

1. **Znovu spočítá hash zprávy** (pomocí stejné hashovací funkce).
2. Pomocí tvého veřejného klíče a matematických vztahů (modulární aritmetiky) ověří, zda podpis (hodnoty rrr a sss) odpovídá hashi.

Pokud chceš šifrovat a dešifrovat zprávy, použiješ **RSA**, protože umí obojí – zašifruje zprávu tvým veřejným klíčem, kterou pak dešifruješ svým soukromým klíčem, a naopak. RSA je univerzální, takže kromě šifrování umožňuje i digitální podepisování, což z něj dělá všestranný algoritmus. Na druhou stranu, pokud potřebuješ **jen digitálně podepisovat dokumenty nebo ověřovat jejich pravost**, použiješ **DSA**, který je pro tento účel navržený a optimalizovaný – zprávu nepřímo podepisuje tvým soukromým klíčem a příjemce ji ověřuje tvým veřejným klíčem.