Afina šifra

Afina šifra je poseban slučaj supstitucijske šifre sa dva parametra a i b

Afina šifra se smatra poboljšanom verzijom Cezarove, ali u principu ima jednake slabosti jer je lako dešifrirati metodom učestalosti slova.

- Afina šifra je poseban slučaj supstitucijske šifre sa dva parametra ***a*** i ***b***.
  - ✓ neka su $x,y,a,b \in \mathbb{Z}26$
  - ✓ Enkripcija $e_k(x) = y \equiv a \cdot x + b \bmod 26$
  - ✓ Dekripcija $d_k(y) = y \equiv a \cdot x + b \bmod 26$

$$a \cdot x + b \equiv y \bmod 26$$
$$a \cdot x \equiv (y - b) \bmod 26$$
$$x \equiv (y - b) \bmod 26/a$$
$$x \equiv a^{-1} \cdot (y - b) \bmod 26$$

1. **Primer**: *Šifrirajte opvoreni tekst* **RADAR** *ako je dat ključ* K=(7,3)
Rešenje:
Kako je redosled pojavljivanja slova u abecedi: R→17, A→0 i D→3
imamo da je: $17 * 7 + 3 = 18 \pmod{26} \rightarrow$ S
$0 * 7 + 3 = 3 \pmod{26} \rightarrow$ D
$3 * 7 + 3 = 24 \pmod{26} \rightarrow$ Y

2. Ako je K = (7, 3) šifrirajte otvoreni tekst MIRKO koristeći Afinov algoritam.

REŠENJE:

$$12 \cdot 7 + 3 \equiv 87 \pmod{26} = 9 \rightarrow \text{J}$$
$$8 \cdot 7 + 3 \equiv 59 \pmod{26} = 7 \rightarrow \text{H}$$
$$17 \cdot 7 + 3 \equiv 122 \pmod{26} = 18 \rightarrow \text{S}$$
$$10 \cdot 7 + 3 \equiv 73 \pmod{26} = 21 \rightarrow \text{V}$$
$$14 \cdot 7 + 3 \equiv 101 \pmod{26} = 23 \rightarrow \text{X}$$

pa je šifrat **JHSVX**.

3. ✓ Dekripcija $d_k(y) = y \equiv a \cdot x + b \bmod 26$

$$a \cdot x + b \equiv y \bmod 26$$
$$a \cdot x \equiv (y - b) \bmod 26$$
$$x \equiv (y - b) \bmod 26/a$$
$$x \equiv a^{-1} \cdot (y - b) \bmod 26$$

- Najlakše je da odredimo broj ***b*** elemenata iz funkcije enkripcije, a to su: 0,1,2,3...25 $\#b = 26$
- Pogledom na Afinu funkciju enkripcije zaključujemo da nema uslova i ograničenja za elemente ***a*** tako da ih možemo brojati kao **b** elemente
- Razlika je što ***a*** nema istu funkciju u dekripciji odnosno koristimo inverzni ***a*** parametar što rezultuje ograničenjem broja elemenata **a**.
- Uslov koji važi za ***a*** elemente je korišćenje **NZD (*a*,26) = 1**.

NZD označava najveći zajednički delilac argumenata u zagradi. Kako je 2·13 = 26, a NZD (aa,26) = 1, za elemente parametra $aa \in \mathbb{Z}$ važe sledeći brojevi: 1,3,5,7,9,11,15,17,19,21,23,25.

Uzmemo li za parametar b 26 brojeva iz skupa $\mathbb{Z}26$ a za parametar mogućih 12 brojeva, množenjem tih dva elemenata dobijemo Afinu šifru sa 312 različitih ključeva → 26 ·12 = 312, # $k\ k$ = 312