Azərbaycan Milli Elmlər Akademiyası
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

2014-cü il oktyabr ayı üçün məsələlər

Bu ayın kriptoqrafik müsabiqəsi **affin şifrlər**ə əsaslanır.

Affin şifr *birəlifbalı əvəzləmə şifrləri*nə aiddir. Affin şifr belə işləyir. Əlifbanın hər bir hərfi müəyyən ədədlə əvəzlənir, sadə riyazi funksiya istifadə edilməklə şifrlənir və alınmış ədədlər yenidən hərflərlə əvəzlənir.

Azərbaycan əlifbasının hərflərini şifrləmək üçün $(ax + b) \bmod 32$ funksiyası istifadə edilir, burada x – hərfin ədədi qarşılığı, a və b seçilmiş ədədlərdir (şifrin açarıdır).

Deşifrləmə funksiyası $a^{-1}(y - b) \bmod 32$ şəklində olacaq, a^{-1} ilə a ədədinin 32 moduluna görə multiplikativ tərsi işarə edilir.

a-nın seçilməsinə məhdudiyyət var: a ədədi 32 ilə qarşılıqlı sadə olmalıdır. Buna görə a-nın mümkün qiymətləri 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29 və 31-dir. b isə 0-dan 31-ə kimi ixtiyari ədəd ola bilər.

A	B	C	Ç	D	E	Ə	F	G	Ğ	H	X	I	İ	J	K
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Affin şifrlərdə modulyar arifmetika (hesab) istifadə edilir. Modulyar arifmetika qalıqlı bölmə ilə əlaqəlidir və yalnız bölmə əməlində alınan qalığa baxılır. Natamam qismət nəzərə alınmır. Tutaq ki, a ədədinin n ədədinə bölünməsindən alınan qalıq r ədədidir. Bu əməliyyat $a \bmod n = r$ kimi işarə edilir.

Məsələn, 27 mod 5 = 2; 64 mod 8 =0.

Mənfi ədədlərin də qalıqlı bölünməsinə baxmaq olar, bu zaman qalığın üzərinə bölünəni gəlməklə nəticəni müsbət etmək olar:

-18 mod 14 = 10 (çünki -18 mod 14 = -4 = (-4 +14) mod 14 = 10).

Ədədlərin cəminin, fərqinin və hasilinin də modula görə nəticəsinə baxmaq olar.

(17+27) mod 15 = 44 mod 15 = 14.

(12-22) mod 15 = -10 mod 15 = 5.

(3×9) mod 15 = 27 mod 15 = 12.

Məsələ 1: **Multiplikativ tərsin hesablanması**

Affin şifrləmənin deşifrləmə funksiyasında modula görə *multiplikativ tərs* qiymətdən istifadə edilir.

Verilmiş n moduluna görə a ədədinin multiplikativ tərsi elə b ədədinə deyilir ki, $(a \times b) \bmod n = 1$ şərtini ödəsin (Multiplikativ tərsin varlığı üçün ƏBOB$(a, b) = 1$ olmalıdır).

Məsələn:

$3^{-1} \bmod 32 = 11$ (çünki $3 \times 11 \bmod 32 = 33 \bmod 32 = 1$);

$5^{-1} \bmod 32 = 13$ ($5 \times 13 \bmod 32 = 65 \bmod 32 = 1$);

$7^{-1} \bmod 32 = 23$ ($7 \times 23 \bmod 32 = 161 \bmod 32 = 1$);

$9^{-1} \bmod 32 = 25$ ($9 \times 25 \bmod 32 = 225 \bmod 32 = 1$).

Azərbaycan əlifbasında mətnləri şifrləmək üçün aşağıdakı multiplikativ tərs qiymətləri də hesablayın:

$11^{-1} \bmod 32 =$ $13^{-1} \bmod 32 =$

$15^{-1} \bmod 32 =$ $17^{-1} \bmod 32 =$

$19^{-1} \bmod 32 =$ $21^{-1} \bmod 32 =$

$23^{-1} \bmod 32 =$ $25^{-1} \bmod 32 =$

$27^{-1} \bmod 32 =$ $29^{-1} \bmod 32 =$

Məsələ 2: ***Affin şifrlə şifrləmə***

Aşağıda açarı $a = 7$ və $b = 4$ olan affin şifrlə açıq mətnin ilk iki hərfinin şifrlənməsi göstərilib. Şifrləməni davam etdirin və şifrmətni tapın.

Açıq mətn	A	F	F	İ	N	Ş	İ	F	R
x	0	7	7	13	19	25	13	7	23
$7x + 4$	4	53							
$(7x + 4) \bmod 32$	4	21							
Şifrmətn	D	Ö							

Məsələ 3: ***Affin şifrlə deşifrləmə***

Aşağıda açarı $a = 19$ və $b = 3$ olan affin şifrlə şifrlənmiş mətnin ilk iki hərfinin deşifrlənməsi göstərilib. Deşifrləməni davam etdirin və açıq mətni tapın.

Şifrmətn	Ç	Q	Ö	S	P	Ç	V	Ğ	Ç	I
y	3	16	21	24	22	3	29	9	3	12
$19^{-1}(y - 3)$	0	351	486							
$19^{-1}(y - 3) \bmod 32$	0	31								
Açıqmətn	A	Z								