Azərbaycan Milli Elmlər Akademiyası
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

2014-cü il mart ayı üçün məsələlər

Məsələ 1: ***Marşrut şifri ilə təbrik***

Marşrut şifrindən (düzbucaqlı cədvəl) istifadə etməklə bayram təbriki şifrlənib. Açarın bir hissəsinin (sütünların nömrələrinin) 7, 5, 3,... olduğunu bilərək təbriki oxuyun.

```
BNRUM BVRMN AIƏOY ZKRAÜ ZIA
```

Məsələ 2: ***Sezar şifrinin qohumu***

Aşağıdakı kriptoqram Sezar şifrində olduğu kimi əlifbanı dövri sürüşdürməklə alınmış şifrləmə əlifbası ilə şifrlənib. Açıq mətnin azərbaycan dilində olduğunu bilərək onu tapın.

```
FƏİYG FEĞFT ŞOSSO ISŞSİ YFPFX IŞOEF ZNOTJ UYŞFZ
OEFBI MTUSU KOEFS FYNOT ZBOBC BCPVO VBUKY FJOEF
ISIPB YUTOŞ ƏF
```

Məsələ 3: ***Məcidin şifri***

Məcid bir şifrləmə üsulu icad edib (onun Vernam şifrindən xəbəri yoxdur). Azərbaycan dili əlifbasının hərfləri 0-dan başlayaraq əlifba sırası ilə ardıcıl nömrələnir və nömrələr ikilik say sistemində 5 bitlə göstərilir: A→ 0 → 00000_2; B→ 1 → 00001_2; …, Z → 31→ 11111_2.

Açar ardıcıllığı $a_1 = b$, $a_n = 3a_{n-1} + 1 \bmod 32$, $n > 1$ düsturu ilə hesablanır və hər bir hədd yuxarıdakı qayda ilə 5 bitlə göstərilir. Fikir verin ki, b-ni dəyişməklə başqa açar alınır. Şifrləmə açıq mətnin və açarın uyğun simvollarının bitləri 2 modulu üzrə toplamaqla (XOR əməli) aparılır. Məsələn, açıq mətn ZAB → 11111 00000 00001 olsun. Açarı generasiya etmək üçün b =1 götürsək, $a_1 = 1 \rightarrow 00001_2$; $a_2 = 4 \rightarrow 00100_2$ və $a_3 = 13 \rightarrow 01101_2$ alarıq.

Şifrlənmiş mətn 11111 + 00001 = 11110 (30_{10} →**Y**); 00000 +00100 = 00100 (4_{10} →**D**); 00001+01101 = 01100 (12_{10} →**I**).

Bu şifrlə şifrlənmiş mətn **GƏHMLLHZSB** olarsa, açıq mətni tapın.