TIK-110.503 Kryptologian perusteet
Loppukoe
29.1.2000

1. Kuka on se keksijä joka nimesi uuden keksintönsä kuuluisan selviytyjän

   ```
   RLD ABLAIORXBLJ
   ```

   mukaan? Ainakin osaat määrätä keksijän nimikirjaimet joita on käytetty avaimena kun selviytyjän nimi, joka alkaa kirjaimilla `RO`, on salattu **affiinilla menetelmällä**. Käytetyn aakkoston merkit ovat 26 kirjainta `A - Z` sekä sanaväli, ja ne on muutettu kokonaisluvuiksi modulo 27 seuraavan taulukon mukaan:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	"väli"
13	14	15	16	17	18	19	20	21	22	23	24	25	26

2. Selväkieli muodostuu toisistaan riippumattomista biteistä, jotka on ryhmitelty kahdeksan bitin lohkoiksi. Nolla-bitin todennäköisyys selväkielessä on p. Jokainen lohko $x_1, x_2, \ldots, x_8$ salataan käyttäen yhtä avainbittiä z joka lasketaan yhteen modulo 2 lohkon jokaisen selväkielibitin kanssa. Siis salakielilohko on $y_1, y_2, \ldots, y_8$ missä $y_i = x_i \oplus z$, $i = 1, 2, \ldots, 8$. Kuten tavallista oletetaan että avainbitit generoidaan satunnaisesti ja selväkielestä riippumatta. Oletetaan että satut näkemään salakielilohkon jossa on k nollabittiä ja $8 - k$ ykkösbittiä, missä $k = 0, 1, 2, \ldots, 8$. Määrää todennäköisyys sille että avainbitti on $z = 0$. Mikä salakielilohko maksimoi tämän todennäköisyyden?

3. a) Esitä Solovay-Strassenin alkulukutesti parittomalle kokonaisluvulle n, $n > 1$.

   b) Onko 21 Eulerin pseudo-alkuluku kannan 2 suhteen?

4. Luku 29 on luvun 841 neliöjuuri. Määritä joku toinen luku joka on luvun 841 neliöjuuri modulo 2000. Opastus: Jos m_1 jakaa luvun $a - b$ ja m_2 jakaa luvun $a + b$, ja jos $\gcd(m_1, m_2) = 1$, niin $a^2 \equiv b^2 \pmod{m_1 m_2}$.

5. Tarkastellaan **ElGamalin Julkisen Avaimen Salausmenetelmää** Galois'n kunnassa $\mathrm{GF}(2^4)$ kun polynomina on $x^4 + x + 1$ ja primitiivialkiona $\alpha = 0010 = x$. Salainen avaimesi on $a = 7$.

   a) Laske julkinen avaimesi β.

   b) Tulkitse salakieliteksti (0100,1110) salaisen avaimesi avulla. Muistathan että kun selväkieli on $X \in \mathrm{GF}(2^4)^*$ niin salakieli on $(\alpha^k, X\beta^k)$ missä kokonaisluku k on vain salaajan tiedossa.