Setning

Allar tölur má skrifa: $b_m 2^n + b_{m-1} 2^{n-1} + \cdots + b_2 2^2 + b_1 2 + b_0$, Þar sem öll $b_i \in \{0, 1\}$.

Dæmi:

$27 = 16 + 8 + 2 + 1 = 2^4 + 2^3 + 2^1 + 2^0 = 11011_2$.

Endurtekin ferningun (*repeated squaring*)

Dæmi:

$3^{11} = 3^{8+2+1} = ((3^2)^2)^2 \cdot 3^2 \cdot 3 \pmod 5$ $3^2 \equiv 9 \equiv 4 \pmod 5$ $(3^2)^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod 5$ $((3^2)^2)^2 \equiv 1^2 \equiv 1 \pmod 5$ svo: $3^{11} \equiv 1 \cdot 4 \cdot 3 \equiv 12 \equiv 2 \pmod 5$

XOR-Dulkóðun

Bókstöfum er breytt í tvíundatölur, t.d $a = 0000$, $b = 0001$ o.s.f.v.. Til að dulkóða skilaboð er notaður lykilstraumur sem er bara runa af tvíundatölum t.d. $1110100101010101010\ldots$.

Bókstöfunum okkar er XOR-að við lykilstrauminn og útkoman eru dulkóðuðu skilaboðin.

Til að afkóða skilaboðin er þeim aftur XOR-að við lyilstrauminn og svo breytt í bókstafi aftur.

RSA-reikniritið (*Með fyrirvara um villur því ég missti af fyrirlestrinum*)

Veljum tvær prímtölur p og q. Látum $n = p \cdot q$.

Veljum tölu e sem er ósamþátta $(p-1)(q-1)$, og tölu $d = e^{-}1 \pmod{(p-1)(q-1)}$

Til að dulkóða tölu m, reiknum við $m^e \pmod n$.

Til að afkóða tölu s reiknum við $s^d \pmod{\text{n}}$.

Dæmi.

Tölusetjum stafrófið svo

A	B	C	D	E	F	G	H	I	J
02	03	04	05	06	07	08	09	10	11
K	L	M	N	O	P	Q	R	S	T
12	13	14	15	16	17	18	19	20	21
U	V	W	X	Y	Z	Þ	Æ	Ö	
22	23	24	25	26	27	28	29	30	

Dulkóðum “BJÖRK” $= 3, 11, 30, 19, 12$ með $n = 34 \implies p = 2, q = 17$ og $e = 3$

$B = 3^3 \equiv 27 \pmod{34} \to Z$

$J = 11^3 \equiv 5 \pmod{34} \to D$

$\text{Ö} = 30^3 \equiv 4 \pmod{34} \to C$

$R = 19^3 \equiv 25 \pmod{34} \to X$

$K = 12^3 \equiv 26 \pmod{34} \to \text{Þ}$