korabbi kepletek:

$$p \text{ prim}, 1 < a, b < p, n \in \mathbb{Z}, g \text{ generator}$$
$$\log_g(a \cdot b) = \log_g a + \log_g b \pmod{p-1}$$
$$\log_g(a^n) = n \cdot \log_g a \pmod{p-1}$$

Deffie-Hellman

A, $a \in \mathbb{Z}_{p-1}$	publikus p, g	B, $b \in \mathbb{Z}_{p-1}$

A elkuldi g^a-t, B elkuldi g^b-t

B kiszamolja: $(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$
A kiszamolja: $\left(g^b \bmod p\right)^a \bmod p = g^{ba} \bmod p$

feladat

$$p = 11, g = 2, a = 3, b = 4$$

A: $2^3 \bmod 11 = 8$, $5^3 \bmod 11 = 4$		B: $2^4 \bmod 11 = 5$, $8^3 \bmod 11 = 4$

todo megoldas

RSA

p, q primek, $n = p \cdot q$

$e \geq 2, \text{lnko}(e, \varphi(n)) = 1$

$\left(\varphi(n) = p \cdot q \cdot \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1)\right)$

$$d : e \cdot d \equiv 1 \mod \varphi(n)$$
$$(ax \equiv b \bmod n)$$
$$\text{Titkos kulcs} : (p, q, d), \quad \text{publikus kulcs} : (n, e)$$
$$n \text{ uzenet}, 1 \leq m < n, \text{lnko}(m, n) = 1$$
$$c = m^e \bmod n \quad m = c^d \bmod n \quad (\text{c a cypher valami})$$

feladat

$p = 11, q = 13, e = 7$

$b = ?, c = ?$ ha $\mod 4$

$$n = p \cdot q = 11 \cdot 13 = 143$$
$$\varphi(n) = (11-1)(13-1) = 120$$
$$d:$$
$$e \cdot d \equiv 1 \mod \varphi(n)$$
$$7d \equiv 1 \mod 110$$

120	x	1	0
7	x	0	1
1	17	1	-17
0	7	-7	120

$$7d \equiv (1-7k)120 + (-17+120k)7$$
$$7d \equiv (-17+120k)7 \mod 120$$
$$7d \equiv -17 \cdot 7 \mod 120$$
$$d \equiv -17 \mod 120$$
$$d \equiv 103$$

c = ?

$$c = m^e \mod n = 4^7 \mod 143 = 4^4 \cdot 4^3 \mod 143 = 256 \cdot 16 \cdot 4 \mod 143 = 113 \cdot 64 \mod 143 = 82$$

gyakorlas

$$205^{206^{207}} \mod 103 = ?$$
$$a^{\varphi(n)} \mod n$$
$$\varphi(103) = 102 \Longrightarrow$$
$$\Longrightarrow 205^{102} \mod 103 = 1$$
$$205^{207} \mod 103 = 205^{102+102+1} \mod 103 = 205^{2 \cdot 102+1} \mod 103 = 205^{2 \cdot 202} \cdot 205 \mod 103 = 105 \mod 103 = 2$$

$$a^k \mod n = a^{k \mod \varphi(n)} \mod n, \text{ ha } (a,n) = 1$$

1

150 forint visszajaro, hanyfelekeppen kaphatjuk meg ha huszas es otvenes van csak

$$150 = 20x + 50y$$

50	x	1	0
20	x	0	1
10	2	1	-2
0	2	-2	5

$$10 = (1-2k)50 + (-2+5k)20$$
$$150 = (15-30k)50 + (-30+75k)20$$

2

13 szorosat felirva 4-es szamrendszerben 21-re vegzodik a szam

$$13x \equiv 2 \cdot 4^1 + 1 \cdot 4^1 \bmod 4^1$$

$$13x \equiv 9 \bmod 16$$

16	x	1	0
13	x	0	1
3	1	1	-1
1	4	-4	5
0	3	13	-16

$$3 = (1 + 13k)16 + (-1 - 16k)13$$

$$9 = (3 + 13k)16 + (-3 - 16k)13$$

$$13x = (-3 - 16k)13 \quad \bmod 16$$

$$13x \equiv -3 \cdot 13 \quad \bmod 16$$

$$x \equiv -3 \quad \bmod 16$$

$$x \equiv 13 \quad \bmod 16$$

$$x \equiv 13$$

$$x \equiv 29$$