«به نام خدا»

تکلیف چهارم – مرضیه علیدادی – 9631983

---

1. Let X1 and X2 be any 2 solutions to the system of congruences. Note that:

$$X1 \equiv X2 \equiv a \pmod{m1}$$

Thus, m1|(X1−X2). By a similar reasoning, mi|(X1−X2) for i=1,2. Therefore, if [m1,m2] denotes the least common multiple (LCM) of m1,m2, then:

$$[m1,m2] \mid (X1-X2)$$

Since m1,m2 are relatively prime, [m1,m2]=m1m2. Therefore,

$$m1m2 \mid (X1-X2)$$

$$X1 \equiv X2 \pmod{m1m2}$$

This means that any two solutions must be congruent modulo m1m2. It follows that the system of congruences has at most 1 solution modulo m1m2.

---

2. p-1 positive multiples of a:

$$a,\ 2a,\ 3a,\ \dots\ (p-1)a$$

Suppose that ra and sa are the same modulo p, then we have r = s (mod p), so the p-1 multiples of a above are distinct and nonzero; that is, they must be congruent to 1, 2, 3, ..., p-1 in some order. Multiply all these congruences together and we find

$$a\,(2a)\,(3a)\,\dots\,((p-1)a) \equiv 1\cdot2\cdot3\cdot\dots\cdot(p-1) \pmod{p}$$

which is, $a^{(p-1)}(p-1)! \equiv (p-1)! \pmod{p}$. Then divide both side by (p-1):

$$a^{p-1} \equiv 1 \pmod{p}$$

Then multiply by a:

$$a^{p} \equiv a \pmod{p}$$

If k is an integer satisfying 1≤k≤p−1, then k!=1⋅2⋅3⋯k is a product of positive integers smaller than p, and therefore k! is not divisible by p. For the same reason, if 1≤k≤p−1 then (p−k)!=1⋅2⋅3⋯(p−k) is not divisible by p. Since p! obviously is divisible by pp, we infer that

$\binom{p}{k} = \frac{p!}{k!(p-k)!} \equiv 0$ mod p whenever 1≤k≤p−1.

Therefore

$(x+y)^p = x^p+y^p+\sum_{k=1}^{p-1}\binom{p}{k}x^k a^{p-k} \equiv x^p+y^p$ mod p.

---

3. 1 is a weak value to use as a private key because the published public key will be equal to α, which allows an attacker to infer the private key.

p − 1 is also a weak value because α p−1 mod p ≡ 1 for any α since p is a prime number, which would also allow an attacker to infer the private key.

4.

4.1. $k_{pubA} \equiv \alpha^a \bmod p \equiv 2^{228} \bmod 467 \equiv 394$ $\qquad 228_2 = 11100100$

$k_{pubB} \equiv \alpha^b \bmod p \equiv 2^{57} \bmod 467 \equiv 313$

$k_{AB} \equiv (k_{pubA})^b \bmod p = 394^{57} \bmod 467 = 206$

4.2. $k_{pubA} = \alpha^a \bmod p \equiv 4^{400} \bmod 467 = 89$

$k_{AB} = (k_{pubA})^b \bmod p \equiv 89^{134} \bmod 467 = 161$

4.3. Are they???

5.

11: $\phi(11) = 10 \rightarrow 2, 6, 7, 8$

6.

Bob's public key: we have $b = a^d \equiv 40909 \pmod p$, so Bob's public key is (p, a, b) = (44927, 7, 40909)

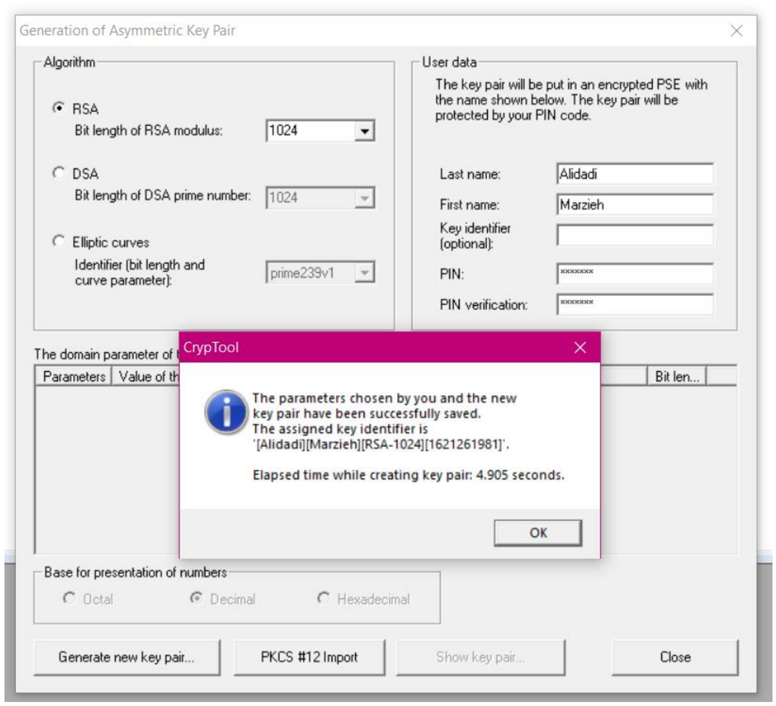
To encode, we choose a random k with 0 < k < p − 1: = 6708.

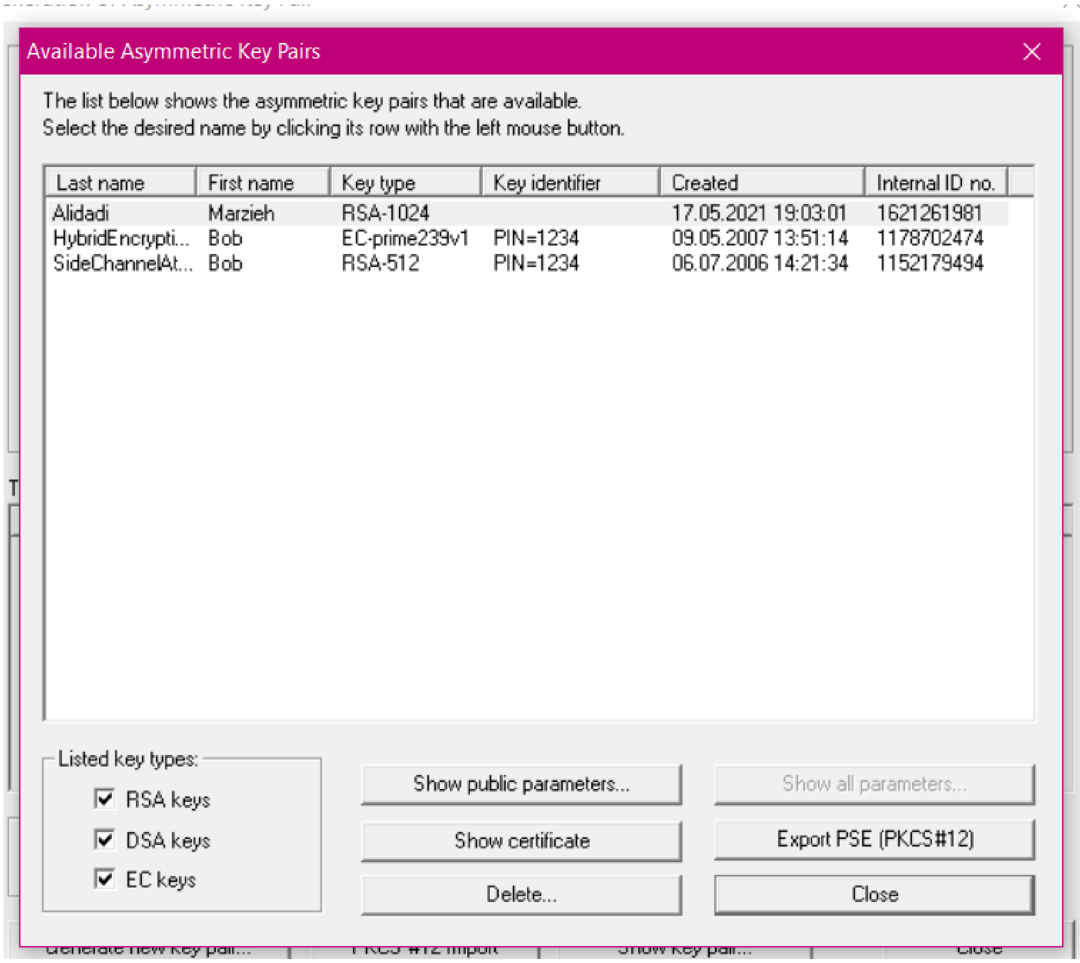
We then compute $r = a^k \equiv 12510 \pmod p$ and $t = b^k m \equiv 12749 \pmod p$, so the ciphertext Alice sends Bob is: (r, t) = (12510, 12749)

To decrypt, Bob computes $r^{-d} \equiv 11355 \pmod p$ and multiplies it by t to obtain the result m = 10101.

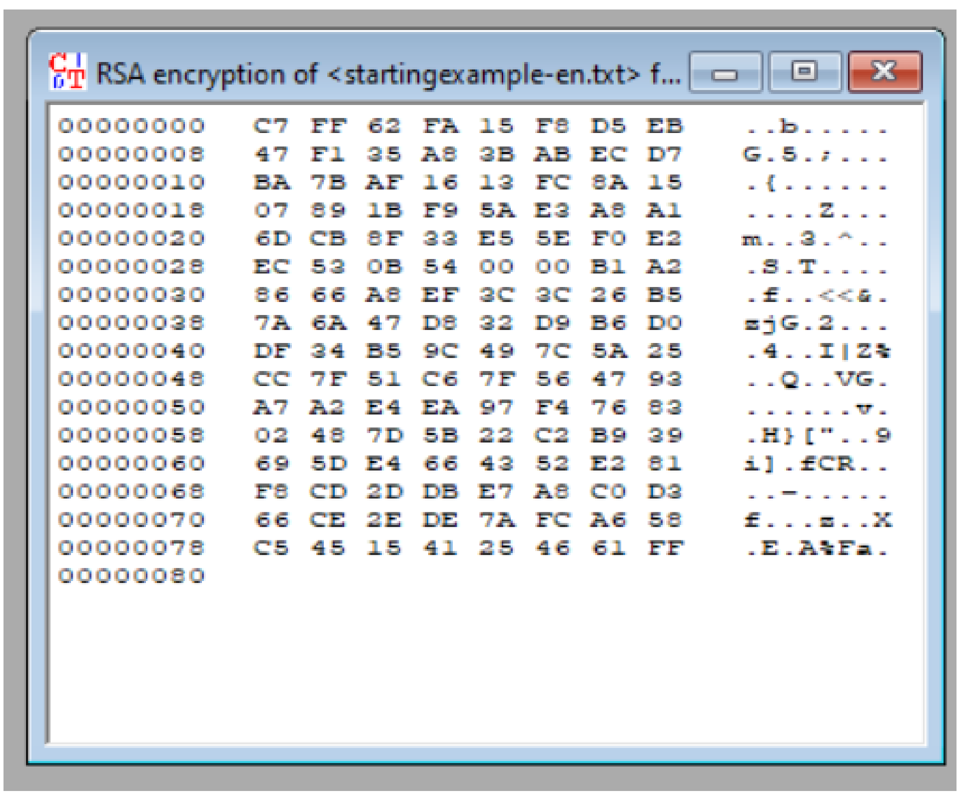
7.

3.

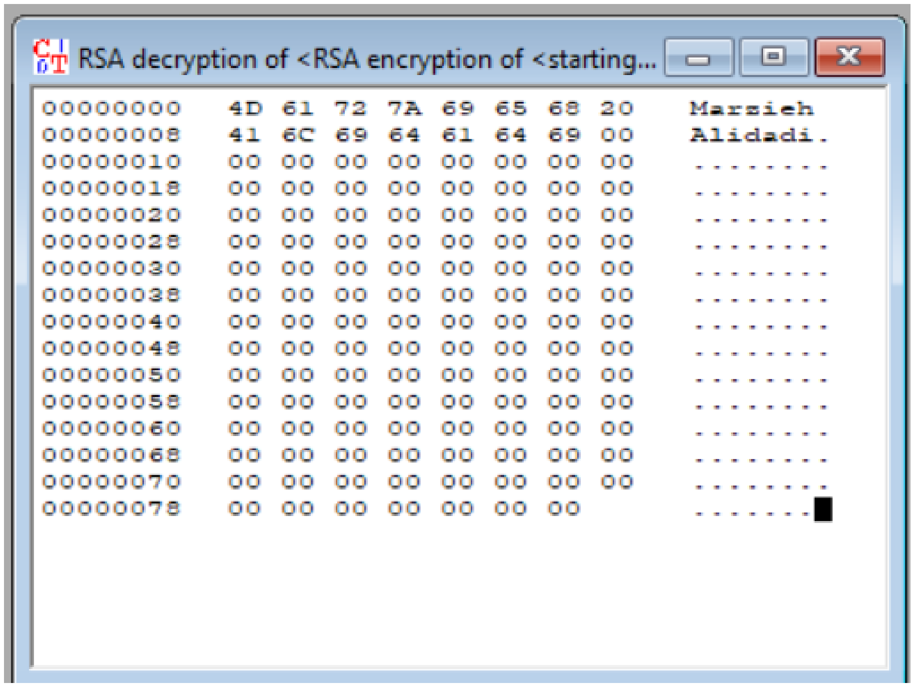



Available Asymmetric Key Pairs
The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.
Last name | First name | Key type | Key identifier | Created | Internal ID no.
Alidadi | Marzieh | RSA-1024 | | 17.05.2021 19:03:01 | 1621261981
HybridEncrypti... | Bob | EC-prime239v1 | PIN=1234 | 09.05.2007 13:51:14 | 1178702474
SideChannelAt... | Bob | RSA-512 | PIN=1234 | 06.07.2006 14:21:34 | 1152179494
Listed key types:
RSA keys
DSA keys
EC keys
Show public parameters...
Show all parameters...
Show certificate
Export PSE (PKCS#12)
Delete...
Close

4. encrypted:


RSA encryption of <startingexample-en.txt> f...
00000000 C7 FF 62 FA 15 F8 D5 EB
00000008 47 F1 35 A8 3B AB EC D7
00000010 BA 7B AF 16 13 FC 8A 15
00000018 07 89 1B F9 5A E3 A8 A1
00000020 6D CB 8F 33 E5 5E F0 E2
00000028 EC 53 0B 54 00 00 B1 A2
00000030 86 66 A8 EF 3C 3C 26 B5
00000038 7A 6A 47 D8 32 D9 B6 D0
00000040 DF 34 B5 9C 49 7C 5A 25
00000048 CC 7F 51 C6 7F 56 47 93
00000050 A7 A2 E4 EA 97 F4 76 83
00000058 02 48 7D 5B 22 C2 B9 39
00000060 69 5D E4 66 43 52 E2 81
00000068 F8 CD 2D DB E7 A8 C0 D3
00000070 66 CE 2E DE 7A FC A6 58
00000078 C5 45 15 41 25 46 61 FF
00000080

Decrypted:



8. OPTIONAL

we have an algorithm that can decrypt an arbitrary ElGamal ciphertext (r, t) with associated public key (p, a, b) to produce the message $m \equiv t \cdot r^{-\log_a b} \pmod p$,

and we wish to break a Diffie-Hellman problem of computing the value $g^{xy} \pmod p$ given the values (p, g, c_x, c_y) where $c_x = g^x \pmod p$, $c_y = g^y \pmod p$.

To do this, give the ElGamal algorithm the data (p, a, b, r, t) with $a = g$, $b = c_x$, $t = 1$, and $r = c_y$:

it will output the message $m = 1 \cdot (g^y)^{-\log_g (g^x)} \equiv g^{-xy} \pmod p$.

Then $g^{xy} \equiv m^{-1} \pmod p$ can be computed immediately.

Conversely, suppose we have an algorithm that can break an arbitrary Diffie-Hellman problem of computing the value $g^{xy} \pmod p$ given the values (p, g, c_x, c_y) where $c_x = g^x \pmod p$, $c_y = g^y \pmod p$, and we wish to decrypt an arbitrary ElGamal ciphertext (r, t) with associated public key (p, a, b) to produce the message $m \equiv t \cdot r^{-\log_a b} \pmod p$.

To do this, give the Diffie-Hellman algorithm the data (p, g, c_x, c_y) where $g = a$, $c_x = b$, and $c_y = r$:

it will then output the value $c_x^{\log_g c_y} = b^{\log_a r} = b^k$. We can then compute $m \equiv t \cdot b^{-k} \pmod p$ immediately.