1) $24^{66,000,000,023} \pmod{77}$

Use chinese Remainder theorem, where $n=77$

$p=7, q=11$, so

$24^{66,000,000,023} \pmod 7$, $24^{66,000,000,023} \pmod{11}$

From Fermat's little theorem.

if a is integer, p is prime in $a^p = a \pmod p$

then $a^{p-1} \equiv 1 \bmod (p)$

So,

$24^{7-1} \bmod 7 = 1 \bmod 7$

raise the power to 11000000003

$\longrightarrow (a^m)^n = a^{m \times n}$

$24^{66000,000,018} \equiv 1 \bmod 7$

$24^{66000000018} \times 24^5 = 24^5 \bmod 7$

$24^{66,000,000,023} = 7962624 \bmod 7$

so, $24^{10} \bmod 11 \equiv 1 \bmod 11$

raise the power to 66,000,000,02

$24^{66,000,000,020} \bmod 11 \equiv 1 \bmod 11$

$24^{66,000,000,020} \times 24^3 = 24^3 \bmod 11$

From above we get $x = 8 \bmod 11$

$x = 5 \bmod 7$

using chineare remainder theorem

$$x = (a_1 m_1 y_1 + a_2 m_2 y_2) \bmod M$$

Here $M = 77$, $m_1 = 7$, $m_2 = 11$

we know $m_1 y_1 \equiv 1 \bmod 11$ $\quad m_2 y_2 \equiv 1 \bmod 7$

$y_1 = m_1^{-1} \bmod 11$ $\quad y_2 = m_2^{-1} \bmod 7$

$y_1 = 8$ $\quad y_2 = 2$

$$x = (8 \times 7 \times 8 + 5 \times 11 \times 2) \bmod 77$$

$$x = (8 \ 448 + 110) \bmod 77$$

$$x = 558 \bmod 77$$

$$x = 19$$

$\therefore \quad 24^{661,000,000,023} \pmod{77} = 19$

2) ElGamal :-

In decryption, to get plain text we use

$$x = y_2 (y_1^a)^{-1} \bmod p.$$

number to alphabets :-

For encryption, we have value $= x26^2 + y26 + z$

For deryption, we have to find x, y, z, which are respective Alaphebets.

$x = \text{Round}(n/26^2)$

$y = \text{Round}(n - x26^2/26)$

$z = (n - x26^2) - (26y)$

Prem chand avanigadda

ELGamal cryptosystem

Enter a:7899

Enter p:31847

Enter alpha val:5

Enter cipher file name to decrypt: ELGamalCiphertext.txt

Shestandsupinthegardenwhereshehasbeenworkingandlooksintothedistanceshehassensedachangeinthe weatherthereisanothergustofwindabuckleofnoiseintheairandthetallcypressesswaysheturnsandmovesup hilltowardsthehouseclimbingoveralowwallfeelingthefirstdropsofrainonherbarearmsshecrossestheloggia andquicklyentersthehouse

Final result:

She stands up in the garden where she has been working and looks into the distance. She has sensed a change in the weather. There is another gust of wind, a buckle of noise in the air, and the tall cypresses sway. She turns and moves uphill towards the house. Climbing over a low wall, feeling the first drop of rain on her bare arms, she crosses the loggia and quickly enters the house.

3) 5.11

a) let take $y_1^{c_1}(y_2^{c_2})^{-1}$ ——— (1)

we know $y_1 = x^{b_1} \bmod n$

$y_2 = x^{b_2} \bmod n$

replace y_1 and y_2 in (1)

$\Rightarrow (x^{b_1})^{c_1}((x^{b_2})^{c_2})^{-1}$ $\boxed{(a^m)^n = a^{mn}}$

$\Rightarrow x^{b_1 c_1}(x^{b_2 c_2})^{-1}$ $\boxed{a^m \times a^n = a^{m+n}}$

$\Rightarrow x^{b_1 c_1 - b_2 c_2}$

we know from fact $c_2 \equiv (c_1 b_1 - 1)/b_2$

$c_2 b_2 \equiv c_1 b_1 - 1$

$1 \equiv c_1 b_1 - c_2 b_2$

$\Rightarrow x^1$

$\Rightarrow x$.

$\therefore x \equiv y_1^{c_1}(y_2^{c_2})^{-1} \bmod n.$

b) $n = 18721$, $b_1 = 43$, $b_2 = 7717$, $y_1 = 12677$

$y_2 = 14702$

step 1:- $c_1 \leftarrow b_1^{-1} \bmod b_2$

$c_1 \leftarrow 43^{-1} \bmod 7717$

$c_1 \equiv 2692$

$c_2 \leftarrow (c_1 * b_1 - 1)/b_2$

$c_2 \equiv (2692 * 43 - 1)/7717$

$c_2 \leftarrow 15$

$x \leftarrow y_1^{c_1} (y_2^{c_2})^{-1} \bmod n$

$x \equiv 12677^{2692} (14702^{15})^{-1} \bmod 18721$

By Sloving above, we will get

$x = 15001$

4) results:

x in alpha:799

y in alpha:790
1. number of points: 504
2. largest point: (1035, 854)
3. is (1014, 291) belong to E: No

x in beta:385

y in beta:749
ElGamal public key
1.encryption
2.decryption
3.quit

Enter choice:1
Enter plain text

x in plaintext:575

y is plaintext:419
encrypted result ((523, 790), (935, 290))
ElGamal public key
1.encryption
2.decryption
3.quit

Enter choice:2
b value 340

enter x in y1 cipher:873

enetr y in y1 cipher:233

enter x in y2 cipher:234

enetr y in y2 cipher:14
decrypted result (413, 233)
ElGamal public key
1.encryption
2.decryption
3.quit

Enter choice:3
Diffie-hellman key exchange

enter x in alpha:818

enter y in alpha:121

enter x in A:199

enter y in A:72

enter x in B:815

enter y in B:519

4) Diffe-hellman

$A = a\alpha \quad B = b\alpha$

find a and b using α, double point

$$\text{key} = bA$$
$$= b(a\alpha)$$

6) Private key = {a}, Public key = {P, α, β}

$$\beta = \alpha^a$$

we know sig(m) = {λ, Δ}

$$\lambda = \alpha^k$$
$$\Delta = k^{-1}(m - a\lambda)$$

we know $\Delta = 0$

$$m = a\lambda$$

So, $m = a\alpha^k$

$$a = m(\alpha^k)^{-1}$$

If we keep $\Delta = 0$, then Attaker may crack private key a.