Date 11-5-21
Page

ASSIGNMENT-2

Information System Security

By-
Amit Kumar Sahu
18MIS7250

Under Guidance of-
Prof. Saroj Kumar Panigrahy

Note*: For the 1st Question, the solution is on last page that is a java program.

1) Use the Fermat's method to find the factors of 127.

$$x = \sqrt{n} = \sqrt{127} = \lfloor 11.27 \rfloor$$
$$= 12$$

iteration	x	$w = x^2 - n$	is w perfect square	$y = \sqrt{w}$	a	b
1.	12	$144 - 127 = 17$	No	-	-	-
2.	13	$169 - 127 = 42$	No	-	-	-
3.	14	$196 - 127 = 69$	No	-	-	-
4.	15	$225 - 127 = 98$	No	-	-	-
5.	16	$256 - 127 = 129$	No	-	-	-
6.	17	$289 - 127 = 162$	No	-	-	-
7.	18	$324 - 127 = 197$	No	-	-	-
8.	19	$361 - 127 = 234$	No	-	-	-
9.	20	$400 - 127 = 273$	No	-	-	-
10.	21	$441 - 127 = 314$	No	-	-	-
11.	22	$484 - 127 = 357$	No	-	-	-
12.	23	$529 - 127 = 402$	No	-	-	-
13.	24	$576 - 127 = 449$	No	-	-	-
14.	25	$625 - 127 = 498$	No	-	-	-
15.	26	$676 - 127 = 549$	No	-	-	-
16.	27	$729 - 127 = 602$	No	-	-	-

Since its taking so much time to calculate. Ive will be programming this method.

Note*

All the programming codes are at the end of this assignment.

Also we got 1 and 127 after 53 iterations after using the program which tells that 127 is a perfect prime number.

2.

The miller Rabin Test takes a candidate integer n as input and returns the result "composite" if n is definitely not a prime, and the result "inconclusive" if n may or may not be prime.

If this algorithm is repeatedly applied to a number and repeatedly returns "inconclusive", then the probability that the number is actually prime increases with each inconclusive test.

The probability required to accept number as a prime can be set as close to 1.0 as desired by increasing the number of tests performed.

3.

Miller-Rubin Test

$$n-1 = m \times 2^k$$

$$a^{n-1} = a^{m \times 2^k} = [a^m]^{2^k} = [a^m]^{k \text{ times}}$$

Let $a = 1$

If $1^q \bmod n = 1$

then return ("inconclusive").

Clearly in Test it returns ("inconclusive"). ⇒ #Step 3 of Algorithm

Considering $a = n-1$

for $j = 0$

the test is if $(n-1)^q \bmod n = n-1$

then return ("inconclusive").

This condition is met by day zon ⇒ #Step 5 of Algorithm

Hence both are inconclusive which proves that both $a=1$ and $a(n-1)$ are inconclusive.

4.

Show that 2047 is a strong pseudoprime to the base 2.

In 1st step of 2047 Miller-Rabin Test

$k = 1$ and $q = 1023$

$(2047 - 1) = (2)^1 (1023)$

In 2nd step we select $a = 2$ as the base.

In 3rd step we have $a^q \bmod n = 2^{1023} \bmod 2047$

$2^{1023} \bmod 2047 = (2^{11})^{93} \bmod 2047$

since $n - 1 = m \times 2^k \Rightarrow 1024 - 1 = 2^{10} \cdot m \Rightarrow 93 \times 11 = 1023$

$(2^{11})^{93} \bmod 2047 = (2048)^{93} \bmod 2047 = 1$

And therefore the test is passed.

$\therefore 2^{11} = 2047$ and $\frac{1023}{11} = 93$ so $11 \times 93 = 1023$

5.

a) Find $3^{201} \bmod 11$

Using Fermat's Theorem

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

If p is prime and a is a positive integer not divisible by p.

Therefore $3^{201} = (3^{10})^{20} \times 3 = 3 \pmod{11}$

$= 3$

b) no. btw 0 and 72 with a congruent g^{794} modulo 73

Since from Fermat's theorem. $a^{p-1} \equiv 1 \pmod{p}$

$g^{72} \equiv 1 \pmod{73}$ ——— (1)

So: $g^{794} = g^{72 \times 10 + 74} \bmod 73$

$= (g^{72})^{10} \times g^{74} \bmod 73$

From eq? (1)

$= 1 \times g^{74} \bmod 73$

$= g^{(72+2)} \bmod 73$

$= g^{72} \cdot g^{2} \bmod 73$

$= 81 \bmod 73$

$= 8$

c) Number between 0 and 28 with x^{85} congruent to 6 modulo 29.

$$x^{85} = 6 \mod (29)$$

We can write

$$\frac{x^{85}}{6} = 1 \mod (29)$$

By Fermat's little theorem if a is not divisible by a prime P, then $a^{p-1} = 1 \mod p$

This satisfies if we keep $x = 6$;

$$\frac{6^{85}}{6} = 6^{84} = (6^3)^{28} = 6^3$$

$$(6^3)^{28} = (6^3)^{29-1} \equiv 1 \mod 29$$

So the number is 6

6.

a) Find a number n between 0 and 9 such that n is congruent to 7^{1000} modulo 10.

$$n \equiv 7^{1000} \bmod 10$$

Euler's theorem 2nd version

$$a^{\phi(n+1)} = a \pmod n$$

By Euler's Totient

$$\phi(10) = 4 \qquad (1, 3, 5, 7)$$

Therefore $7^4 \equiv 1 \pmod{10}$ by Euler's theorem

therefore

$$7^{1000} = (7^4)^{250} \equiv (1)^{250} \equiv 1 \bmod 10$$

Hence the number is 1.

b) Find a number x between 0 and 28 with x^{85} congruent to 6 modulo 35

$$x^{85} \equiv 6 \pmod{35}$$

By Fermat-Euler's theorem

$a^{\phi(n)} \equiv 1 \bmod n$

for $n = 35$, $\phi(35) = ?$

There are 10 positive integers from 1 to 34 which are not coprime with 35, which are {5, 7, 10, 14, 15, 20, 21, 25, 28, 30}.

Therefore which are coprime $= 34 - 10 = 34 - 10$
$= 24$

So $\phi(35) = 24$

$x^{\phi(35)} \equiv x^{24} \equiv 1 \bmod 35$

or else we can do this ↓

$x^{85} \equiv 6 \pmod 5 \equiv 1$ ∴ $35 = 5 \cdot 7$

$\gcd(5, 7) = 1$

$\phi(5) = 4, 85 \equiv 1 \pmod 4$; $x \equiv (1 \bmod 5)$ ——— (1)

$x^{85} = 6 \pmod 7$

$\phi(7) = 6, 85 \equiv 1 \pmod 6$; $x \equiv 6 \pmod 7$ ——— (2)

Applying Chinese Remainder theorem;

$x \equiv 1 \pmod 5$

$x \equiv 6 \pmod 7$

// $M_1 = M = 7 \times 5 = 35$ $\quad a_1 = 1$, $a_2 = 6$

$M_1 = \frac{35}{5} = 7$ $\qquad M_2 = \frac{35}{7} = 5$

$7^{-1} \bmod 5 = 3$

$5^{-1} \bmod 7 = 5^{-1} \bmod 7 = 3$

$m_1 = \frac{M}{M_1}$

$m_2 = \frac{M}{M_2} =$

~~$x = 1 \cdot 7 \times 2 + 6 \times 5 \times 3$~~

It is clear that $x = 6$ by observation

$x \equiv 6 \bmod 35$

$= 6$

$6^{85} \equiv 6 \pmod{35}$

$= 6$

$x = (a_1 M_1 x_1 + a_2 M_2 x_2)$

$= 1 \cdot 7 \cdot 3 + 6 \cdot 5 \cdot 3$

$= 111 \bmod 35$

$= 6 \bmod 35 = 6$

7.

a) $\phi(41)$

Since 41 is a prime number so by Eulers totient's function $\phi(p) = p - 1$

so $\phi(41) = 41 - 1 = 40$

b) $\phi(27)$

$\phi(27) = \phi(3^3)$ since 3 is prime

By Euler's totient formula

$\phi(p^e) = p^e - p^{e-1}$ if p is a prime

$\phi(3^3) = 3^3 - 3^{3-1} = 3^3 - 3^2 = 27 - 9$

$= 18$ //

c) $\phi(231)$

By Euler's totient formula

$\phi(m \times n) = \phi(m) \times \phi(n)$

$\phi(231) = \phi(3) \times \phi(7) \times \phi(11)$ $[\phi(p) = p-1]$ p = prime

$= (3-1) \times (7-1) \times (11-1)$

$= 2 \times 6 \times 10 = 120$ //

3	231
7	77
11	11
	1

$231 = 3 \times 7 \times 11$

d) $\phi(440) =$

By Euler's totient formula

$\phi(m \times n) = \phi(m) \times \phi(n)$

$\phi(440) = \phi(2^3) \times \phi(5) \times \phi(11)$

$= (2^3 - 2^2) \times (5-1) \times (11-1)$

$= 4 \times 4 \times 10$

$= 16 \times 10$

$= 160$ //

2	440
2	220
2	110
5	55
11	11
	1

8.

$x \equiv 4 \bmod 6$

$x \equiv 3 \bmod 5$

Using chinese Remainder Theorem.

$M = 6 \times 5 = 30$

$M_1 = \frac{30}{6} = 5$ $\qquad$ $M_2 = \frac{30}{5} = 6$

$m_1 = 5^{-1} \bmod 4 = 1$

$m_2 = 6^{-1} \bmod 3 = 0$

28 is the smallest possible number of coins that meet the condition. $4 \cdot 7 = 28$.

So

$28 \bmod 7 = 0$

Hence 0 coins left when they are divided among 7 people.

or $y = 4 \pmod 6$

$y \equiv 3 \pmod 5$

division algorithm

$y = 6n + 4$

$6n \equiv 4 \pmod 5$

$n \equiv 4 \pmod 5$

$n = 5q + 4$

Means $y = 30q + 28$

$y \equiv 28 \pmod{30}$

$28 \div 7 = 4$, our remainder is 0 //

9.

Let the smallest positive integer be x

Given $x_1 = 1 \bmod 5$ $\quad a_1 = 1$ $\quad m_1 = 5$

$x = 2 \bmod 4$ $\quad a_2 = 2$ $\quad m_2 = 4$

$x = 3 \bmod 7$ $\quad a_3 = 3$ $\quad m_3 = 7$

$M = m_1 \times m_2 \times m_3 = 5 \times 4 \times 7 = 140$

$M_1 = \frac{M}{m_1} = \frac{140}{5} = 28$ $\quad M_2 = \frac{140}{4} = 35$ $\quad M_3 = \frac{M}{m_3} = \frac{140}{7} = 20$

$M_i x_i \equiv 1 \pmod{m_i}$

$M_1 x_1 \equiv 1 \pmod{m_1}$

$28 x_1 \bmod 5 = 1$

$\boxed{x_1 = 3}$

since $28 \times 3 = 84$ by hit & trial

$M_2 x_2 \equiv 1 \pmod{m_2}$

$35 x_2 \bmod 4 = 1$

by hit & trial

$35 \times 3 = 105$

$\boxed{x_2 = 3}$

$M_3 x_3 \equiv 1 \pmod{m_3}$

$20 x_3 \bmod 7 = 1$

$\boxed{x_3 = 1}$

Now $x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \bmod M$

$= (28 \times 3 \times 1 + 35 \times 3 \times 2 + 20 \times 1 \times 3) \bmod 140$

$= (84 + 210 + 60) \bmod 140$

$= 354 \bmod 140$

$= 74 \bmod 140$

Since want smallest so $74 \bmod 140$ can also be written as $66 \bmod 140$ which is equal to $\underline{66}$ (Ans)

10.

Using Euler's Totient function.

$$\phi(p^e) = p^e - p^{e-1} \text{ if } p \text{ is a prime}$$

$$\phi(25) = \phi(5^2) = 5^2 - 5^{2-1}$$
$$= 25 - 5 = 20$$

We know that 2 is a primitive root.

The others are 2^i where i is relatively prime to $\phi(25)$

$$\phi(\phi(25)) = \phi(20) = 4 \times 2 = 8$$

So there are 8 primitive roots.

Now neglecting 1, 4, 9 & 16 by using the definition of prime root.

& $6^{10} = 1 \pmod{25}$, $10 < \phi(25)$

Which leads to 6 is not primitive root of 25

Similarly $14^{10} \equiv 1 \pmod{25}$, $10 < \phi(25)$

$19^{10} \equiv 1 \pmod{25}$, $10 < \phi(25)$

We get the prime roots of 25 as

2, 3, 8, 12, 13, 17, 22, 23

11.

$p = 397 \quad q = 401 \quad e = 343$

$M = "NO"$ plain text = 13 14

$n = pq = 397 \times 401 = 159197$

$\phi(n) = \phi(p \cdot q) = \phi(p) * \phi(q) = (397-1) \times (401-1)$
$= 396 \times 400$
$= 158400$

[By Euler's totient function]

Encryption but before that calculating d

$de = 1 \bmod \phi(n)$

$d = e^{-1} \bmod \phi(n)$

$s = s_1 - q s_2$

$t = t_1 - q t_2$

By using Extended Euclidean theorem

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
461	158400	343	277	1	0	1	0	1	-461
1	343	277	66	0	1	-1	1	-461	462
4	277	66	13	1	-1	5	-461	462	-2309
5	66	13	1	-1	5	-24	462	2309	12007
13	13	1	0						
	1	0							

$t = -461 - 4(462) = -2309$

$t = 462 - 5(-2309)$

$= 11545 + 462$

$= 12007$

So $d = 12007$

Encryption: $C = P^e \bmod n$

$1314^{343} \bmod 159197$

Using Fast Exponentation

$343 = 101010111_2$.

$343 = 2^0 + 2^1 + 2^2 + 2^4 + 2^6 + 2^8$

2	343	1
2	171	1
2	85	1
2	42	0
2	21	1
2	10	0
2	5	1
2	2	0
2	1	1
	0	

$1314 \bmod 159197 = 1314$

$1314^2 \bmod 159197 = (1314^1 \times 1314^1) \bmod 159197$

$= (1314^1 \bmod 159197)(1314^1 \bmod 159197) \bmod 159197$

$= (1314)(1314) \bmod 159197$

$= 1726596 \bmod 159197$

$= 134626$

$1314^4 \bmod 159197 = (1314^2 \bmod 159197)(1314^2 \bmod 159197) \bmod 159197$

$= (134626 \times 134626) \bmod 159197$

$= 1.812416 \times 10^{10} \bmod 159197$

$= 59017$

$1314^6 \bmod 159197 = (1314^2 \bmod 159197)(1314^4 \bmod 159197) \bmod 159197$

$= (134626 \times 59017) \bmod 159197$

$= 7945222642 \bmod 159197$

$= 18766$

$1314^8 \bmod 159197 = (1314^6 \bmod 159197)(1314^2 \bmod 159197) \bmod 159197$

$= (18766 \times 134626) \bmod 159197$

$= 2526391516 \bmod 159197$

$= 94323$

$1314^{343} \bmod 159197 = (1314^1 \bmod 159197 \times 1314^2 \bmod 159197 \times$
$1314^4 \bmod 159197 \times 1314^6 \bmod 159197$
$\times 1314^8 \bmod 159197) \bmod 159197$

$= (1314 \times 134626 \times 59017 \times 18766 \times 94323) \bmod 159197$

$= 6.72447509 \times 10^{21} \bmod 159197$

$= 1.847952288 \times 10^{22} \bmod 159197$

Ciphertext = 33, 677

Decryption:

$P. = 33677^{12007} \bmod 159197$

Using Fast Exponentiation

$12007_{10} = 10111011100111_2$

$12007 = 2^0 + 2^1 + 2^2 + 2^5 + 2^6 + 2^7 + 2^9 + 2^{10} + 2^{11} + 2^{13}$

2	12007	1
2	6003	1
2	3001	1
2	1500	0
2	750	0
2	375	1
2	187	1
2	93	1
2	46	0
2	23	1
2	11	1
2	5	1
2	2	0
2	1	1
	0	

$33677 \bmod 159197 = 33677$

$33677^2 \bmod 159197 = (33677 \bmod 159197) \times (33677 \bmod 159197) \bmod 159197$

$= (33677 \times 33677) \bmod 159197$

$= 1134140329 \bmod 159197$

$= 20901$

$33677^5 = (20901 \times 20901 \times 33677) \bmod 159197$

$= 2.834189303 \times 10^4 \bmod 159197$

$= 33609$

$33677^6 = (33677 \bmod 159197)(33677^5 \bmod 159197) \bmod 159197$

$= (33677 \times 33609) \bmod 159197$

$= 1131850293 \bmod 159197$

$= 118820$

$33677^7 = (33677^6 \bmod 159197)(33677^1 \bmod 159197) \bmod 159197$

$= (118820 \times 33677) \bmod 159197$

$= 4001501140 \bmod 159197$

$= 84545$

$33677^9 = (33677^8 \bmod 159197)(33677^2 \bmod 159197) \bmod 159197$

$= (84545 \times 20901) \bmod 159197$

$= 1767075045 \bmod 159197$

$= 147542$

$33677^{10} = (33677^9 \bmod 159197)(33677 \bmod 159197) \bmod 159197$

$= (147542 \times 33677) \bmod 159197$

$= 4968771934 \bmod 159197$

$= 74367$

$33677^{11} = (33677^{10} \bmod 159197)(33677 \bmod 159197) \bmod 159197$

$= (74367 \times 33677) \bmod 159197$

$= 2504457459 \bmod 159197$

$= 129452$

$33677^{13} = (33677^{11} \bmod 159197)(33677^2 \bmod 159197) \bmod 159197$

$= (129452 \times 20901) \bmod 159197$

$= 2705676252 \bmod 159197$

$= 123237$

$$33677^{12007} = (33677^{1} \times 33677^{2} \times 33677^{5} \times 33677^{6} \times 33677^{7} \times 33677^{9} \times 33677^{10} \times 33677^{11} \times 33677^{13}) \pmod{159147}$$

$$= (33677 \times 20901 \times 33609 \times 118820 \times 8455 \times 147542 \times 74367 \times 129452 \times 183237) \pmod{159147}$$

$$= 4.138159905 \times 10^{42} \pmod{159147}$$

$$= 1314$$

Hence again decryption is $1314 =$ "NO"

12. Rabin Cryptosystem

$p = 23$ and $q = 7$

$p \equiv q \equiv 3 \pmod 4$

$n = p \times q = 23 \times 7 = 161$ $\quad n$ = public key

Plaintext = 24 = m

2	24	0
2	12	0
2	6	0
2	3	1
2	1	1
	0	0

$24_{10} = 11000_2$

Encryption: $C = m^2 \bmod n$

$= 24^2 \bmod 161$

$= 576 \bmod 161$

$= 93$

So the ciphertext to be send is 93

Decryption: By Chinese Remainder theorem ✓

∴ { ~~Extended Euclidean Algorithm such that $a \cdot p + b \cdot q = 1$~~ } not needed ✗

$a_1 = +(C^{(p+1)/4}) \bmod p = +(93^{(23+1)/4}) \bmod 23$

$a_2 = -(C^{(p+1)/4}) \bmod p = -(93^{(23+1)/4}) \bmod 23$

$b_1 = +(C^{(q+1)/4}) \bmod p = +(93^{(7+1)/4}) \bmod 23$

$b_2 = -(C^{(q+1)/4}) \bmod p = -(93^{(7+1)/4}) \bmod 23$

$a_1 = 1 \bmod 23$

$a_2 = 22 \bmod 23$

$b_1 = 4 \bmod 7$

$b_2 = 3 \bmod 7$

Four possible answers (a_1, b_1), (a_1, b_2), (a_2, b_1) and (a_2, b_2)

(a_1, b_1) $\quad x = 1 \bmod 23$ $\qquad$ GCD $(7, 23) = 1$

$x = 4 \bmod 7$

here $a_1 = 1$, $a_2 = 4$; $m_1 = 23$, $m_2 = 7$

$M = m_1 \times m_2 = 23 \times 7 = 161$

$M_1 = \frac{M}{m_1} = 7$ $\qquad$ $M_2 = \frac{M}{m_2} = 23$

$M_i x_i \equiv 1 \pmod{m_i}$

$M_1 x_1 \equiv 1 \pmod{m_1}$

$7 x_1 \pmod{23} = 1$

By hit and trial $\quad 23 \times 4 = 92$ & $13 \times 7 = 91$

$\boxed{x_1 = 13}$

Similarly $\quad M_2 x_2 = 1 \pmod{m_2}$

$23 x_2 = 1 \pmod 7$ $\qquad$ $23 \times 4 = 92$ & $13 \times 7 = 91$

$\boxed{x_2 = 4}$

$x = (M_1 x_1 a_1 + M_2 x_2 a_2) \bmod M$

$= (7 \times 13 \times 1 + 23 \cdot 4 \cdot 4) \bmod 161$

$x = (91 + 3684) \bmod (61)$

$= 459 \bmod (61)$

$= 137$

For (a_1, b_1) := plaintext = 137

Similarly (a_2, b_2) By CRT

$x = 22 \bmod 23$

$x = 4 \bmod 7$

$a_1 = 22, \quad a_2 = 4, \quad m_1 = 23, \quad m_2 = 7$

$M = 23 \times 7 = (61)$

$M_1 = \frac{M}{m_1} = 7 \qquad M_2 = \frac{M}{m_2} = 23$

$M_1 X_1 \equiv 1 \pmod{m_1}$

$7 X_1 \equiv 1 \pmod{23}$

$X_1 = 13$

$M_2 X_2 \equiv 1 \pmod{m_2}$

$23 X_1 \equiv 1 \pmod{7}$

$X_2 = 4$

$x = (M_1 X_1 a_1 + M_2 X_2 a_2) \bmod M$

$= (7 \cdot 13 \cdot 22 + 23 \cdot 4 \cdot 4) \bmod 161$

$= (2370) \bmod 161$

$= 116$

For (a_2, b_2) = plaintext = 116

(a_1, b_2) By CRT

$X = 1 \bmod 23$

$X = 3 \bmod 7$

$a_1 = 1$, $a_2 = 3$, $m_1 = 23$, $m_2 =>$

$M = 161$

$M_1 = 7$ $M_2 = 23$

$X_1 = 13$ $X_2 = 4$

$x = (M_1 X_1 a_1 + M_2 X_2 a_2) \bmod M$

$= (7 \times 13 \times 1 + 23 \cdot 4 \cdot 3) \bmod 161$

$= 367 \bmod 161 = 367 \bmod 161 = \underline{45}$

(a_2, b_2) By CRT

$X = 22 \bmod 23$

$X = 3 \bmod 7$

$a_1 = 22$, $a_2 = 3$, $m_1 = 23$, $m_2 = 7$

$M = 161$, $M_1 = 7$, $M_2 = 23$, $X_1 = 13$, $X_2 = 4$

$x = (M_1 X_1 a_1 + M_2 X_2 a_2) \bmod 161$

$= (7 \cdot 13 \cdot 22 + 23 \cdot 4 \cdot 3) \bmod 161$

$= 2278 \bmod 161 = \underline{24}$

Here we will consider (a_2, b_2) which is the plaintext.

13.) RSA-based Digital Signature Scheme

$p = 167 \quad q = 113 \quad e = 201 \quad M = "hi"$

$M = 78$

$n = p \times q = 167 \times 113$

$= 18871$

$\phi(18871) = 167 \times 113 = (167-1) \times (113-1) = 166 \times 112$

$= 18592$

$ed = 1 \bmod \phi(n)$

$d = e^{-1} \bmod \phi(n) = 201^{-1} \bmod 18592$

By using extended euclidean method

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
92	18592	201	100	1	0	1	0	1	-92
2	201	100	1	0	1	-2	1	-92	185
100	100	1	0	1					
	1	0							

$d = 185$

$s = s_1 - q s_2$

$t = t_1 - q t_2$

Signing $S = M^d \bmod n$

S = signature M = message

$S = 78^{185} \bmod 18871$

2	185	1
2	92	0
2	46	0
2	23	1
2	11	1
2	5	1
2	2	0
2	1	1
	0	

$185 = 10111001_2$

Using Fast Exponentiation

$185 = 2^0 + 2^3 + 2^4 + 2^5 + 2^7$

$78^3 \bmod 18871 = (78 \times 78 \times 78) \bmod 18871$

$= 474552 \bmod 18871$

$= 2777$

$78^4 \bmod 18871 = (78^3 \bmod 18871)(78^1 \bmod 18871) \bmod 18871$

$= (2777 \times 78) \bmod 18871$

$= 216606 \bmod 18871 = 9025$

$78^5 \bmod 18871 = (78^4 \bmod 18871)(78^1 \bmod 18871) \bmod 18871$

$= (9025 \times 78) \bmod 18871$

$= 703950 \bmod 18871 = 5723$

$78^8 \bmod 18871 = (78^5 \bmod 18871)(78^2 \bmod 18871) \bmod 18871$

$= (5723 \times 6084) \bmod 18871$

$= 34818732 \bmod 18871$

$= 15383$

$78^{185} \bmod 1887 = (78^3 \cdot 78^4 \cdot 78^5 \cdot 78^7) \bmod 1887$

$= (2777 \cdot 9025 \cdot 5723 \cdot 15383) \bmod 1887 = 1845766742$

$= 12126 \bmod 1887$

$= 12126$

Verifying

$M = S^e \bmod n$

$= 12126^{201} \bmod n$

$= 12126^{201} \bmod 1887$

$201 = 11001001_2$

$201 = 2^0 + 2^3 + 2^6 + 2^7$

2	201	1
2	100	0
2	50	0
2	25	1
2	12	0
2	6	0
2	3	1
2	1	1
	0	

$12126^2 \bmod 1887 = (12126^1 \bmod 1887)(12126^1 \bmod 1887) \bmod 1887$

$= (12126 \times 12126) \bmod 1887$

$= 146933186 \times 10^{10} \bmod 1887$

$= 18382$

$12126^3 \bmod 1887 = (18382 \times 12126) \bmod 1887$

$= 222900132 \bmod 1887$

$= 14751$

$12126^6 \bmod 1887 = (14751 \times 14751) \bmod 1887$

$= 217592001 \bmod 1887 = 9371$

$12126^7 \bmod 1887 = (12126^6 \bmod 1887)(12126^1 \bmod 1887) \bmod 1887$

$= 9371 \cdot 12126 \bmod 1887$

$= 113632746 \bmod 1887 = 10455$

$12126^{201} = (12126^3 \cdot 12126^6 \cdot 12126^7) \bmod 18871$

$= 14751 \cdot 9371 \cdot 10455 \bmod 18871$

$= 539861646 \bmod 18871$

$= 78 \bmod 18871$

$= 78$

Hence $M^1 = M$ so the sgr is accepted and verified.

---

14. ElGamal-based digital signature scheme

$p = 3119, e_1 = 2, d = 127, r = 307$ Message $M = 320$

p.t.o $e_2 = 2^{127} \bmod 3119 = 1702$ $e_2 = e_1^d$

$c_1 = e_1^r \bmod p$

$= 2^{307} \bmod 3119$

$= 2083 \bmod 3119 = 2083$

$307 = 100110011$

$4^2 \bmod 3119 = 16 \bmod 3119$

$16^2 \cdot 2^1 = 256 \cdot 2 = 512 \bmod 3119$

$512^2 \cdot 2^1 = 26214 \cdot 2 = 524288 \bmod 3119$

$= 296 \bmod 3119$

2	307	1
2	153	1
2	76	0
2	38	0
2	19	1
2	9	1
2	4	0
2	2	0
	1	

14. El Gamal-based digital signature scheme

$p = 3119 \quad e_1 = 2 \quad d = 127 \quad r = 307$

$e_2 = 2^d \bmod 3119 = 2^{127} \bmod 3119$

$127 = 1111111_2$

2	127	1
2	63	1
2	31	1
2	15	1
2	7	1
2	3	1
2	1	1
	0	

Using Fast Exponentiation

1 $\quad 1^2 \cdot 2^1 \bmod 3119 = 2$

1 $\quad 2^2 \cdot 2^1 \bmod 3119 = 8$

1 $\quad 8^2 \cdot 2^1 \bmod 3119 = 128$

1 $\quad 128^2 \cdot 2^1 \bmod 3119 = (16384 \cdot 2) \bmod 3119$

$= 1578$

1 $\quad 1578^2 \cdot 2^1 \bmod 3119 = (2490084 \cdot 2) \bmod 3119$

$= 4980168 \bmod 3119 = 2244$

1 $\quad 2244^2 \cdot 2^1 \bmod 3119 = (5035536 \cdot 2) \bmod 3119$

$= 10071072 \bmod 3119$

$= 2940$

1 $\quad 2940^2 \cdot 2^1 \bmod 3119 = (8643600 \cdot 2) \bmod 3119$

$= 17287200 \bmod 3119$

$= 1702$

$e_2 = 1702$

Signing: $S_1 = e^{\gamma} = 2^{307} \bmod 3119$

$307 = 100110011_2$

2	307	1
2	153	1
2	76	0
2	38	0
2	19	1
2	9	1
2	4	0
2	2	0
2	1	1
	0	

Using Fast Exponentiation.

1 $2^1 \bmod 3119$

0 $4 \bmod 3119$

0 $16 \bmod 3119$

1 $2 \cdot 16^2 \bmod 3119 = (256 \cdot 2) \bmod 3119$
$= 512 \bmod 3119$

1 $2 \cdot 512^2 \bmod 3119 = (262144 \cdot 2) \bmod 3119$
$= 524288 \bmod 3119$
$= 296$

0 $296^2 \cdot 2^0 \bmod 3119 = 87616 \bmod 3119$
$= 2681$

0 $2681^2 \cdot 2^0 \bmod 3119 = (7187761) \bmod 3119$
$= 2681$

1 $2681^2 \cdot 2^1 \bmod 3119 = (7187761 \cdot 2) \bmod 3119$
$= 14375522 \bmod 3119$
$= 51$

1 $51^2 \cdot 2^1 = 2601 \cdot 2 \bmod 3119$
$= 5202 \bmod 3119$
$= 2083 \bmod 3119$

$s_1 = 2083$

$s_2 = (M - d \times s_1) \times r^{-1}$

$= (320 - 127 \times 2083) \times 307^{-1} \mod 3119$

$= [(193 \times 2083) \times 307^{-1}] \mod 3119$

$= (402019 \mod 3119)(307^{-1} \mod 3119) \mod 3119$

$= [2787 \cdot (307^{-1} \mod 3119)] \mod 3119$

Using Extended Euclidean Algorithm

$s_2 = [(320 - 264541) \times (307^{-1})] \mod 3119$

$= (-264221 \mod 3119)(307^{-1} \mod 3119) \mod 3119$

$= [894 \cdot (307^{-1} \mod 3119)] \mod 3119$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
10	3119	307	49	1	0	1	0	1	-10
6	307	49	13	0	1	-6	1	-10	61
3	49	13	10	1	-6	19	-10	61	-193
1	13	10	3	-6	19	-25	61	-193	254
3	10	3		19	-25		-193	254	-955
3	3	1		-25					

$s = 94$ $\quad t = -955$

$t = t_1 - q t_2$

$s = s_1 - q s_2$

$s_2 = 2105 \bmod 3119$ $\boxed{s_2 = 2105}$

Verifying

$v_1 = e_1^M = 2^{320} \bmod 3119$

2^{320} using Fast Exponentiation

$320 = 101000000_2$

1	$2 \bmod 3119$
0	$2^2 \bmod 3119 = 4 \bmod 3119$
1	$2^{16} \bmod 3119 = 32 \bmod 3119$
0	$32^2 \bmod 3119 = 1024 \bmod 3119$
0	$1024^2 \bmod 3119 = 1048576 \bmod 3119 = 592$
0	$592^2 \bmod 3119 = 350464 \bmod 3119 = 1136$
0	$1136^2 \bmod 3119 = 1290496 \bmod 3119 = 2349$
0	$2349^2 \bmod 3119 = 5517801 \bmod 3119 = 290$
0	$290^2 \bmod 3119 = 84100 \bmod 3119 = 3006$

2	320	0
2	160	0
2	80	0
2	40	0
2	20	0
2	10	0
2	5	1
2	2	0
2	1	1
	0	

$\boxed{v_1 = 3006}$

$v_2 = e_2^{s1} \times s_1^{s2} = 1702^{2083} \times 2083^{2105}$

$= \{(1702^{2083} \bmod 3119)[(2083^{2105}) \bmod 3119]\} \bmod 3119$

Calculating using fast exponentiation

$(2083)_2 = 100000100011$

1 $1702 \bmod 3119$

0 $1702^2 \bmod 3119 = 2896804 \bmod 3119 = 2372$

0 $2372^2 \bmod 3119 = 5626384 \bmod 3119 = 2827$

0 $2827^2 \bmod 3119 = 7991929 \bmod 3119 = 1051$

0 $1051^2 \bmod 3119 = 1104601 \bmod 3119 = 475$

0 $475^2 \bmod 3119 = 225625 \bmod 3119 = 1057$

1 $1057^2 \cdot 2072^1 \bmod 3119 = (1117249 \cdot 1702) \bmod 3119 = 187$

0 $187^2 \bmod 3119 = 34969 \bmod 3119 = 660$

0 $660^2 \bmod 3119 = 435600 \bmod 3119 = 2059$

0 $2059^2 \bmod 3119 = 4238481 \bmod 3119 = 760$

1 $1072^1 \cdot 760^2 \bmod 3119 = 983075200 \bmod 3119 = 709$

1 $1072^1 \cdot 709^2 \bmod 3119 = 955563062 \bmod 3119 = 2648$

$2083^{2105} \bmod 3119$

$(2105)_2 = 100000111001_2$

1 $2083 \bmod 3119$

0 $2083^2 \bmod 3119 = 4338889 \bmod 3119 = 360$

0 $360^2 \bmod 3119 = 129600 \bmod 3119 = 1721$

0 $1721^2 \bmod 3119 = 2961841 \bmod 3119 = 1910$

0 $1910^2 \bmod 3119 = 3648100 \bmod 3119 = 1989$

0 $1989^2 \bmod 3119 = 3956121 \bmod 3119 = -1229$

1 $1229^2 \cdot 2083^1 \bmod 3119 = (1510441 \cdot 2083) \bmod 3119$
$= 3146248603 \bmod 3119$
$= 1019$

1 $1019^2 \cdot 2083^1 \bmod 3119 = (1038361 \cdot 2083) \bmod 3119$
$= 2162905963 \bmod 3119$
$= 1104$

1 $1104^2 \cdot 2083^1 \bmod 3119 = (1218816 \cdot 2083) \bmod 3119$
$= 2538793728 \bmod 3119$
$= 2584$

0 $2584^2 \bmod 3119 = 6677056 \bmod 3119 = 2396$

0 $2396^2 \bmod 3119 = 5740816 \bmod 3119 = 1856$

1 $2083^1 \cdot 1856^2 \bmod 3119 = 3444736 \cdot 2083 \bmod 3119$
$= 7175385088 \bmod 3119$
$= 828$

$V_2 = [(1702^{2083} \bmod 3119)(2083^{2105} \bmod 3119)] \bmod 3119$
$= (2648 \times 828) \bmod 3119$
$= 2192544 \bmod 3119$
$= 3006$

Hence $V_1 = V_2 = 3006$, so we can say that the sign is verified.

15. Diffi-Hellman Exchange Key

$g = 97 \quad p = 331 \quad x = 53 \quad y = 67$

$R_1 = g^x \bmod p$

$= 97^{53} \bmod 331$

Using Fast Exponentation

$53 = (110101)_2$

2	53	1
2	26	0
2	13	1
2	6	0
2	3	1
2	1	1
	0	

1 $97 \bmod 331$

0 $97 \cdot 97^2 \bmod 331 = 97^3 \bmod 331$

$= 912673 \bmod 331$

$= 106$

1 $106^2 \bmod 331 = 11236 \bmod 331$

$= 313 \bmod 331$

0 $313^2 \bmod 331 = 98569 \bmod 331$

$= 314 \bmod 331$

1 $314^2 \bmod 331 = 98596 \bmod 331$

$= 289 \bmod 331$

1 $289^2 \cdot 97^1 \bmod 331 = (83521 \cdot 97) \bmod 331$

$= 8101537 \bmod 331$

$= 312 \bmod 331$

$R_1 = 312$

$R_2 = g^y \bmod p$

$= 97^{67} \bmod 331$

$67 = (1000011)_2$

2	67	1
2	33	1
2	16	0
2	8	0
2	4	0
2	2	0
2	1	1
	0	0

1 $97 \bmod 331$

0 $97^2 \bmod 331 = 9409 \bmod 331 = 141$

0 $141^2 \bmod 331 = 19881 \bmod 331 = 21$

0 $21^2 \bmod 331 = 441 \bmod 331 = 110$

0 $110^2 \bmod 331 = 12100 \bmod 331 = 184$

1 $184^2 \cdot 97^1 \bmod 331 = (33856 \cdot 97) \bmod 331$

$= 3284032 \bmod 331$

$= 181$

1 $181^2 \cdot 97^1 \bmod 331 = (32761 \cdot 97) \bmod 331$

$= 3177817 \equiv 217 \bmod 331$

$= 217$

$\boxed{R_2 = 217}$

Verifying keys.

Alice's key

$K = (R_2)^x \bmod p$

$= (217)^{53} \bmod p$ $\quad 53 = (110101)_2$

Using Fast Exponentation.

1 $217^1 \bmod 331$

1 $217^2 \cdot 217^1 \bmod 331 = (47089 \cdot 217) \bmod 331$

$= 10218313 \bmod 331$

$= 12$

0 $12^2 \bmod 331 = 144$

1 $144^2 \cdot 217^1 \bmod 331 = (20736 \cdot 217) \bmod 331$

$= 4499712 \bmod 331$

$= 98$

0 $98^2 \bmod 331 = 9604 \bmod 331$

$= 5$

1 $5^2 \cdot 217^1 = (25 \cdot 217) \bmod 331$

$= 5425 \bmod 331 = 129$

$\boxed{K_1 = 129}$ Alice's key

Now Bob's key will be $K = (R_1)^y \bmod 331$

Using Fast Exponentation $67 = (1000011)_2$

$K = 312^{67} \bmod 331$

1 $312 \bmod 331$

0 $312^2 \bmod 331 = 97344 \bmod 331 = 30$

0 $30^2 \bmod 331 = 900 \bmod 331 = 238$

0 $238^2 \bmod 331 = 56644 \bmod 331 = 43$

0 $43^2 \bmod 331 = 1849 \bmod 331 = 194$

1 $194^2 \cdot 312^1 \bmod 331 = (37636 \cdot 312) \bmod 331$

$= 11742432 \bmod 331 = 207$

I $207^2 \cdot 312^1 \bmod 331 = (42849 \cdot 312) \bmod 331$

$= 13368888 \bmod 331$

$= 129$

$\boxed{K_2 = 129}$ for Bob key

Hence $K_1 = K_2 = 129$ so finally Bob and Alice can exchange keys.