Mission 8

Bharadwaj Thirumal
Coding and Cryptography

December 2, 2016

1. Compute the continued fraction expansion of 83/75

   Solution. The continied fraction expansion is as follows:

$$1 + \frac{8}{75}$$

$$1 + \frac{1}{9 + \frac{3}{8}}$$

$$1 + \frac{1}{9 + \frac{1}{2 + \frac{2}{3}}}$$

$$1 + \frac{1}{9 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}}$$

2. With Digital Signature Algorithm, what happens when you use the same random k twice?

   Solution. If s_A and s_B are the signatures for which the same k is used, then

$$s_A = k^{-1}(H(m_A) + x * r) \ mod \ q$$

$$s_B = k^{-1}(H(m_B) + x * r) \ mod \ q$$

$$s_A - s_B = k^{-1}(H(m_A) + (x * r) - H(m_B) - (x * r))$$

   Cancelling out (x*r) gives,

$$s_A - s_B = k^{-1}(H(m_A) - H(m_B))$$

$$k = \frac{(H(m_A) - H(m_B))}{(s_A - s_B)}$$

   Since the entire signature scheme is based on the value of k being secret, this compromises the scheme.

3. Show the encryption and decryption of the message STOP using RSA with p = 43, q = 59 and e = 13.

   Solution. First, we find $n = p * q = 43 * 59 = 2537$. Then, we process the message STOP into numbers in the ususal way (A = 00, B = 01,..... Z = 25) for our convinience. So STOP becomes 1819 1415. Let us break this into two blocks and encrypt them seperately.

$$1819^{13} \ mod \ 2537 = 2081$$

$$1415^{13} \ mod \ 2537 = 2182$$

So the encrypted message is **C = 2081 2182**

For decryption, we have to find the decryption exponent d which is the inverse of the encryption exponent $e \ mod \ \phi(n)$. Using Eulidean algorithm, we conpute d = 937. Then,

$$2081^{937} \ mod \ 2537 = 1819$$

and

$$2182^{937} \ mod \ 2537 = 1415$$

which is the original message.

4. Solve

$$x \equiv 2 \ mod \ 3,$$

$$x \equiv 3 \ mod \ 5,$$

$$x \equiv 2 \ mod \ 7$$

Solution. We have $m = 3 * 5 * 7 = 105$, and $M_1 = 35, \ m_2 = 21 \ and \ m_3 = 15$. We find that $y_1 = 2$ is the inverse of $M_1 = 35 \ mod \ 3, \ y_2 = 1$ is the inverse of $M_2 \ mod \ 5, \ and \ y_3 = 1$ is the inverse of $M_3 mod \ 7$. Thus the solution of the above system of congruences is,

$$x \equiv (2 * 35 * 2) + (3 * 21 * 1) + (2 * 15 * 1) \ mod \ 105$$

$$= 233 \equiv 23 \ mod \ 105$$

So the solution is $x = 23$.

5. Use Baby step - giant step algorithm to find x so that

$$3^x \equiv \ 2 \ mod \ 29$$

Solution. We should choose m in such a way that $m^2 > 29$. So, let m be 6. We then calculate the two lists:

j	0	1	2	3	4	5
$3^j \pmod{29}$	1	3	9	27	23	11

k	0	1	2	3	4	5
$2 * 3^{-6k} \pmod{29}$	2	15	11	10	17	26

From the tables, we can see that $3^j \pmod{29}$ and $2 * 3^{-6k} \pmod{29}$ have the same value 11 when $j = 5$ and $k = 2$. So,

$$3^5 = 2 * 3^{-12}$$

Rearranging this, we get,

$$3^{17} = 2 \ mod \ 29$$

From this we can see that $x = 17$.

6. Let p be a large prime and α be a primitive root for p. For $m \in \mathbb{Z}$, we define a hash function $h(m) = \alpha^m \ (mod\ p)$.

   (a) Is h pre-image resistant? Why?

   (b) Find a counterexample to prove that h is not strongly collision-free.

   Solution.

   (a) For h to be pre-image resistant, it should be difficult to find $m \in \mathbb{Z}$ for a given $y \in \{1, 2, \ldots, p-1\}$ such that $h(m) = y$. This can be rephrased as follows:
   Find m such that
   $$\alpha^m \equiv y \ (mod\ p)$$
   . This is the discrete log problem and we kknow that currently, it is infeasible to solve it. So h is pre-image resistant.

   (b) Let m_1 and m_2 be two numbers. We know that
   $$m_1 \equiv m_2 \ (mod\ p) \Longrightarrow \alpha^{m_1} \equiv \alpha^{m_2} \ (mod\ p) \Longrightarrow h(m_1) = h(m_2)$$
   Since we can easily pick 2 distinct numbers m_1 and m_2 with $m_1 \equiv m_2 \ (mod\ p)$ which give hashes such that $h(m_1) = h(m_2)$, h is not collision resistant.

7. Jon and Sansa are communicating using the ElGamal cryptosystem with prime $p = 23$ and primitive root $= 7$

   (a) Sansa creates her public key by choosing the exponent $a = 5$. What is Sansa's public key?

   (b) Jon wants to send Sansa, the message '3'. Help Jon encrypt the message.

   (c) Sansa receives an encrypted message $(r, t) = (9, 6)$ from Jon. Help her decrypt the message.

   Solution.

   (a) Sansa's public key is of the form (p, α, β) where $\beta \equiv \alpha^a \ (mod\ p)$.
   So,
   $$\beta \equiv 7^5 \ (mod\ 23) \Longrightarrow \beta \equiv 17 \ (mod\ 23)$$
   .
   Therefore, Sansa's public key is $(23, 7, 17)$

   (b) First, Jon chooses a random number, $k: \ 2 \leq k \leq p-2$. Say Jon chooses $k = 3$.
   Then he calculates
   $$r \equiv \alpha^k \equiv 7^3 \equiv 21 \ (mod\ 23).$$
   Finally
   $$t \equiv \beta^k m \equiv 17^3 * 3 \equiv 19 \ (mod\ 23)$$
   So, Jon sends $(r, t) = (21, 19)$ to Sansa.

   (c) To decrypt, Sansa has to do
   $$tr^{-a} \equiv 6 * 9^{-5} \equiv 18 \ (mod\ 23)$$

8. (a) Factor the RSA number $n = 3844384501$ using the knowledge that
   $$31177611852^2 \equiv 1 \ (mod\ 3844384501)$$

(b) Prove that the number 31803221 is not a prime number using the hint

$$2^{31803212} \equiv 27696377 \ (mod\ 31803221)$$

Solution.

(a) It is given that $31177611852^2 \equiv 1 \ (mod\ 3844384501)$. This implies,

$$(3117761185 - 1) * (3117761185 + 1) \equiv 0 \ (mod\ 3844384501)$$

So,

$$p = gcd((3117761184,\ 3844384501) = 67801$$

and

$$q = p/n = 56701$$

(b) We can see that $2^{n-9} \equiv 27696377 \ (mod\ 31803221)$.
By Fermat's theorem we have, $a^{p-1} \equiv 1 \ (mod\ p)$. To test if Fermat's theorem is true, we multiply the above equation by 2^8.

$$2^{n-9}.2^8 \equiv 27696377 * 256 \equiv 29957450 \neq\ 1 \ (mod\ 31803221).$$

This means that n is not a prime number.

9. Consider the ring given by $(\mathbb{Z}/2\mathbb{Z})/(X^4 + X + 1)$. Find the inverse of $X + 1$

Solution. We can use Extended Euclid's Algorithm to calculate the inverse.

i	q	r	a	b
0	-	$X^4 + X + 1$	0	1
1	-	$X + 1$	1	0
2	X^3	$X^3 + X + 1$	X^3	-
3	1	X^3	$X^3 + 1$	-
4	1	$X + 1$	1	-
5	X^2	1	$X^3 + X^2 + 1$	-

The inverse is $X^3 + X^2 + 1$

10. Use the Miller-Rabin Test to show that 561 is composite.

Solution. We write $n - 1 = 560 = 2^k * m$ with m odd. We find easily that $560 = 2^4 * 35$, so $k = 4$ and $m = 35$. Picking a random number a with $1 < a < 560$, let's pick $a = 3$. Now, let us construct the sequence $b_0, b_1, b_2, b_3 = b_{k-1}$:

$$b_0 \equiv 3^{35} \equiv 78 \ (mod\ 561)$$

$$b_1 \equiv b_0^2 \equiv 474 \ (mod\ 561)$$

$$b_2 \equiv b_1^2 \equiv 276 \ (mod\ 561)$$

$$b_3 \equiv b_2^2 \equiv 441 \ (mod\ 561)$$

Since $b_0 \not\equiv \pm 1 \ (mod\ 561)$ and $b_1, b_2, b_3 \not\equiv -1 \ (mod\ 561)$, the Miller-Rabin test implies that 561 is composite.

11. The number 2 is a primitive root *mod* 29. Use the Pohlig-Hellman algorithm to find $L_2(3)$.

Solution. We write $29-1 = 2^2 * 7$. Let's start with $q = 2$, we see that $(p-1)/q = 14$. The algorithm will yield $y_1 = x_0 + 2x_1$ with each $x_i \in \{0, 1\}$. We first look for x_0 with $2^{14x_0} \equiv 3^{14} \equiv 28 \ (mod\ 29)$, and a simple check by calculator yields $x_0 = 1$.

Let $\beta_1 \equiv 2^{-x_0} * 3 \equiv 16 \ (mod\ 29)$. Next, we search for x_1 with $2^{14x_1} \equiv 16^{(p-1)/q^2} \equiv 16^7 \equiv 1 \ (mod\ 29)$. Therefore we take $x_1 = 0$, and so $y_1 = 1$.

Now we take $q = 7$. We see that $(p-1)/q = 14$. The algorithm yields $y_2 = x_0$ with $x_0 \in \{0, 1, 2, 3, 4, 5, 6\}$. We need x_0 to satisfy $2^{4x_0} \equiv 3^4 \equiv 23 \ (mod\ 29)$. We check the 7 possibilities for x_0 and find $x_0 = 5$ and so $y_2 = 5$.

Finally, we find $x = L_2(3)$ as a simultaneous solution *mod* 28 of the system of congruences

$$x \equiv y_1 \equiv 1 \ (mod\ 4),\ x \equiv y_2 \equiv 5 \ (mod\ 7).$$

Using CRT, we can find a solution $x \equiv 5 \ (mod\ 28)$. Therefore, by Pohlig-Hellman algorithm $L_2(3) = 5$.

12. (a) Divide 2^{10505} by 101 and find the remainder.

Solution. By Fermat's Theorem, $2^{100} \equiv 1 \ (mod\ 101)$. So $2^{10505} \equiv (2^{100})^{105} 2^5 \equiv 1^{105} 2^5 \equiv 32$. The remainder is 32.

(b) What is IND-CPA?

Solution. It is a game where the adversary is given 2 boxes and he knows that there is a random permutation Π and our block cipher E but doesn't know which one is which. The goal is to find out whihc is Π and which is E. This game is called INDistinguishability under Chosen Plaintext Attack (IND-CPA).