CIS 628 Homework 2

Introduction to Cryptography

Saket Kiran Thombre

SU ID: 899913802

NetID: sthombre

Email: sthombre@syr.edu

1. **Use the Euclidean algorithm to compute gcd (30030, 257). Show your work.**

Solution:

To computer the GCD of (30030, 257)

Let's consider 30030 as 'a' and 257 as 'b'

Algorithm:

r = a mod b

let a = b

let b = r

return a till r = 0

let us solve now

r = a mod b

r = 30030 mod 257

r = 218

Now we shift the values to see if r = 0

a = b = 257, b = r = 218, here r is not equal to 0, so we solve further

r = a mod b

r = 257 mod 218

r = 39

Shifting values, a = b = 218, b = r = 39, r is not equal to 0

Therefore, repeat the process

r = a mod b

r = 218 mod 39

r = 23

Now shifting values, a = b = 39, b = r = 23, r is not equal to 0

therefore,

r = a mod b

r = 39 mod 23

r = 16

a = b = 23, b = r = 16, r is not equal to 0

r = a mod b

r = 23 mod 16

r = 7

a = b = 16, b = r = 7, r is not equal to 0 yet,

r = a mod b

r = 16 mod 7

r = 2

a = b = 7, b = r = 2 r is not equal to 0 yet,

r = a mod b

r = 7 mod 2

r = 1

a = b = 2, b = r = 1 r is not equal to 0 yet,

r = a mod b

r = 2 mod 1

r = 0

therefore, we find r = 1

Therefore, we can say that GCD of (30030, 257) is 1.

2. **Compute $18^{489391312}$(mod 19). Show your work.**

Solution:

$18^{489391312}$(mod 19)

= $-1^{489391312}$(mod 19)

= +1(mod 19)

Therefore, $18^{489391312}$(mod 19) = 1.

3. **17^2(Mod 19) is given by**
   a. 6 (mod 19)

b. 4 (mod 19)
c. 8 (mod 19)
d. 17 (mod 19)

Solution:

17^2(Mod 19)

= $(-2)^2$ (mod 19)

= 4 (mod 19)

= b

Therefore 17^2(Mod 19) = 4 (mod 19) = Option B

4. **Find 45^{-1} (mod 46)**

Solution:

As we know, $a^b mod\ c = \ (a\ mod\ c)^b\ mod\ c$, hence, we get

≡ $(45\ mod\ 46)^{-1}\ mod\ 46$

≡ $(-1)^{-1}\ mod\ 46$

≡ -1 $mod\ 46$

≡ 45 mod 46

5. **A solution to the simultaneous set of equations: x ≡ 2 (mod 5) and x ≡ 3 (mod 7) is:**
   a. x ≡17 (mod 35)
   b. x ≡ 6 (mod 35)
   c. x ≡ 6 (mod 7)
   d. Solution does not exist

Solution:

x ≡ 2 (mod 5)

x ≡ 3 (mod 7)

fi	mi	xi

2	7	3
3	5	10

7xi ≡ 1 mod 5

7xi mod 5 ≡ 1 mod 5

5xi ≡ 1 mod 7

5xi mod 7 ≡ 1 mod 7

192 mod 35 ≡ x ≡ 17 mod 35

Therefore,

X ≡ 17 mod 35 = Option A.

6. **Use Chinese Remainder Theorem to solve the following systems of simultaneous equations.**
   x ≡ 2 (mod 4)
   x ≡ 4 (mod 5)
   x ≡ 3 (mod 7)

Solution:

bi	Ni = $\frac{N}{Ni}$	xi	biNixi
2	35	3	210
4	28	2	224
3	20	6	360
			∑ = 794

Step 1:

In Chinese Remainder Theorem, we know that b1 = 2, b2 = 4, b3 = 3

Therefore, xi = bi (mod xi)

Step 2:

Now we have, n1 = 4, n2 = 5, n3 = 7.

From the formula of n, we now know that N1 = n2.n3 and so on for N2 and N3…

So, if we substitute it in the above equation, we get the above values.

Step 3:

For calculating xi, we must perform the following process

x1 = $35^{-1}\ (mod\ 4)$

= 3

Therefore, 105 = 1 mod 4

Hence x1 = 3.

x2 = $28^{-1}\ (mod\ 5)$

= 2

Therefore, 56 = 1 mod 5

Hence x2 = 2.

x3 = $20^{-1}\ (mod\ 7)$

= 6

Therefore, 120 = 1 mod 7

Hence x3 = 6.

Step 4:

We can now further calculate using the formula M = 4.5.7 = 140

x = 794 mod 140

x = 94

We can now further substitute value in the equation to verify value of x,

x = 2 (mod 4)

94 = 2 (mod 4)

Therefore, 94 mod 4 = 2

Similarly, we will check for x = 4 (mod 5)

94 = 4 (mod 5)

Therefore, we get 94 mod 5 = 3

Lastly, x = 3 (mod 7)

94 mod 7 = 3.

From these steps we can conclude that all the substitutions will give the exact remainders for their matching equations respectively.

Therefore, x = 94.

7. **The following question falls in the class of key exchange algorithm**
   Suppose a predetermined key K =1133 is to be shared between Alice and Bob. Alice publishes a number p =12; Alice selects a random number a = 5 (note gcd (a, p-1) =1) and Bob selects a random number b =7 (note gcd (b, p-1) =1).
   a) Alice sends K1 ≡ Ka (mod p) to Bob
   b) Bob sends K2 ≡ K1 b (mod p) to Alice
   c) Alice sends $K3 \equiv K2\ a$ –1 (mod p) to Bob
   d) Bob computes $K \equiv K3\ b$ –1 (mod p)
   Show the calculations for each of the steps a, b, c, and d to determine that Bob gets the correct key.

Solution:

K = 1133, p = 12, a = 5, b = 7

a. Alice will lock the message with a and send it to Bob.
   K1 ≡ $k^a\ (mod\ p)$
   K1 ≡ $1133^5\ (mod\ 12)$
   K1 ≡ $(1133\ mod\ 12)^5\ (mod\ 12)$
   K1 ≡ $5^5\ (mod\ 12)$
   K1 ≡ $5^4.5\ (mod\ 12)$
   K1 ≡ $(25\ mod\ 12)^2\ (5\ mod\ 12)$
   K1 ≡ $1^2\ (5\ mod\ 12)$
   K1 ≡ 5 mod 12
b. Now similarly Bob will lock the message with b and send it to Alice.

K2 ≡ $k^b \ (mod\ p)$
K2 ≡ $5^7 \ (mod\ 12)$
K2 ≡ $5^{2^3}.5 \ (mod\ 12)$
K2 ≡ $(5^2 \ (mod\ 12))^3$. 5 mod 12
K2 ≡ $(25^1 \ (mod\ 12))^3$. 5 mod 12
K2 ≡ 1^3 . $5 \ (mod\ 12)$
K2 ≡ 5

c. Now Alice will remove her lock a and send it back to bob

K3 ≡ $k2^{a^{-1}} \ (mod\ p)$ $\quad$ a^{-1} = x
K3 ≡ $5^7 \ (mod\ 12)$ $\quad$ 5x = 1 mod 12
K3 ≡ 5 $\quad$ x = 7

d. Now Bob will open his lock and calculate K

K ≡ $k3^{b^{-1}} \ (mod\ p)$ $\quad$ b^{-1} = x
Kmod p ≡ $5^5 \ (mod\ 12)$ $\quad$ bx = 1 mod p
1133 mod 12. $5^5 \ (mod\ 12).5^2 \ (mod\ 12)$ $\quad$ 7x = 1 mod 12
5 = 1. $5^2 \ (mod\ 12)$ $\quad$ x = 7
5 = 5

8. Use Diffie-Hellman algorithm to generate key KAB between Alice and Bob using the following numbers. α = 5 p =817; Alice chooses x = 7 and Bob chooses y= 11.

Solution:

α = 5

p =817

Alice	Bob
X = 7	Y = 11
A = $\alpha^x mod\ p$	B = $\alpha^y mod\ p$
A = $5^7 mod\ 817$	B = $5^{11} mod\ 817$
A = 510	B = 120

kA = $B^x \ mod \ p$ kA = $120^7 \ mod \ 817$ kA = 351	kB = $A^y \ mod \ p$ kB = $510^{11} \ mod \ 817$ kB = 351

Hence, we can see that both kA and kB are equal.

Therefore, kA = kB = 351.

Key is 351.

9. **In a network of three users, A, B, and C, we would like to use the Blom scheme to establish session keys between pairs of users. Let p = 31 and let rA = 13, rB = 13, and rC = 2. Suppose Trent (the trusted party) chooses the numbers a = 7, b = 9, and c = 1. Find the session keys KAB and KAC. Show that KAB is the same as KBA. Show your work.4**

Solution:

$a_A = a + \ br_A \ (mod \ p)$

a_A = 7 + 9 * 13 (mod 31)

a_A = 124 (mod 31)

a_A = 0

Now we calculate for b_A

$b_A = b + \ c.r_A \ (mod \ p)$

= 9 + 1 . 13 (mod 31)

= 22 (mod 31)

Now further calculating $K_{AB} \ and \ K_{AC}$

$K_{AB} = g_A \ (R_B)$

$K_{AB} = b_A \ . r_B$ (mod 31)

K_{AB} = 22 * 13 (mod 31)

$K_{AB} = 286\ (mod\ 31)$

$K_{AB} = 7\ (mod\ 31)$

Similarly

$K_{AC} = b_A\ .r_C$ (mod 31)

$K_{AC} = 22 * 2$ (mod 31)

$a_B = a + b.r_B$ (mod p)

$a_B = 7 + 9 * 13\ (mod\ 31)$

$a_B = 124\ \ mod\ 31$

$a_B = 0$

Similarly, we calculated

$b_B = 9 + 1 * 13$ (mod 31)

$b_B = 22$ mod 31

$b_B = 22$

Now we calculate $K_{BA} = g_B\ (R_A)$

$K_{BA} = a_B\ .b_B r$ (mod p)

$K_{BA} = 0\ .b_B r_A$ (mod p)

$K_{BA} = 22 * 13\ (mod\ 31)$

$K_{BA} = 286\ (mod\ 31)$

$K_{BA} = 7\ mod\ 31$

Therefore, we conclude that

$$K_{BA} = K_{AB}$$

10. **What problems the authors propose to solve in 1?**
    a. What changes in the protocol do you suggest if the TPM is implemented as a software solution instead of implementing in a Raspberry PI?
    b. In what way the system is still vulnerable? Propose a solution to the vulnerability you identify. The grade for this question will depend on how you will understand and explain the work proposed.

Solution:

One of the most important security threats is the data exfiltration which happens when a machine is infested with malware. The author mentions a few methods to block data extraction which are currently in use today.

a. Statistical testing base methods
b. Keystroke/mouse click association-based methods
c. Packet marking methods
d. Heuristic rule-based filtering
e. Blacklist based egress filtering
f. Content sensitivity-based filtering

Even with these methods in place, the data exfiltration still takes place. This is a vital limitation that came to light.

The authors hence propose to prevent this data exfiltration problem by implementing a non-interactive dual channel continuous traffic authentication protocol. This new proposed idea will not rely on traditional methods which observe malware behavior or content of information being sent. However, this method will implicitly infer users and consent any outflow of information. The cryptographic hash function will provide the security which will satisfy the preimage and secondary preimage resistance properties. The authors also plan to use dual channels which would authenticate information that is transmitted through the insecure channel. It will also use hashes that are transmitted through an independent narrow band authenticated channel. The protocol designed by the authors will be non-interactive, will require only one-way information flow to verifier. This in turn will make the protocol lightweight for operations and require less frequent authentication.

The authors understand that if human involvement is removed from non-interactive dual channel protocols, they become vulnerable for spoof attacks. Hence, they have also made provisions that will prevent spoof attacks by requiring user to send the user types to the destination IP/Domain name when user sends the first request to the destination. If the user does not comply, the request will be dropped/rejected. The protocol implicitly infers the user's consent from user's normal course of typing. Authors also understand that this requirement would affect user convenience, that's when they also propose protocol extension to address this issue. They also propose second extension to prevent information exfiltration via third party legitimate service providers such as mail servers.

a. **What changes in the protocol do you suggest if the TPM is implemented as a software solution instead of implementing in a Raspberry PI?**

Solution:

Currently the authors have proposed continuous traffic authentication protocol using TPM. This would have a few requirements:

1. Attestation of keystrokes so that we know that they have been generated only using keyboard driver and not by any other application.
2. Interactive protocol operation to setup shared key between client and server. (RSA key exchange)
   For this, we can use a cloud service which will provide a better encryption by providing a computing a bigger shared key. Since raspberry pi is a hardware device, computing a big, shared key will take a lot of time or if we expect a very big key, it won't be able to generate it based on the hardware limitations. Instead, if we use IaaS, we can have a better computing power to do this.
3. There is also a requirement to sign keystroke events. For each authentication request, it makes the use case highly impractical to authenticate the frequent traffic based on authentication requests.
   This impractical part of authenticating the authentication requests can be replaced by using digital signatures. If we replace the raspberry pi with a software, we can implement digital signatures to take over this process.
   Digital signatures are a mathematical scheme for verifying authenticity of digital messages using a valid signature. These digital signatures are part of a robust and in use cryptographical suite created by a known sender to check the integrity of the message.

b. In what way the system is still vulnerable? Propose a solution to the vulnerability you identify. The grade for this question will depend on how you will understand and explain the work proposed.

Solution:

In the conclusion, the authors write that a malware would be able to remove the traffic requests sent through the host by causing a denial-of-service attack, this will in turn deny the legitimate traffic and stop/reduce the productivity of the protocol.

For this, the author can deploy a NGFW (Next-Generation Firewall) in between which will tackle this issue by dropping requests randomly or can create a policy against non-legitimate requests which could be disguised as good traffic. We can also use zone protection against a DoS attack using a NGFW.

Secondly, the authors also assume that the user will not do any malicious activity and type malicious links or domain names.

For this situation, we need to add a firewall and create security rules which will not allow him to communicate with the malicious websites or domain names. This would also trigger an alarm at the system administrator's office. This will help people browse only legitimate traffic if present inside an organization.

Subsequently, most laptops now a days come with a dedicated TPM chip which runs on a separate microprocessor inside the CPU. Timing leakage was discovered in both the Intel firmware based TPM and the TPM chip from STMicroelectronics (fTPM). Both display execution delays that are secret-dependent for producing cryptographic signatures. We show how, even though the key is supposed to be secure inside the TPM hardware, this knowledge allows an attacker to recover 256-bit private keys via digital signature methods based on elliptic curves. On this, Intel upgraded their fTPM firmware which fixed this vulnerability.