Rafid
Shaon
CSC 4222
Nov 28 2022

CSc 4222/6222 Assignment 4
due: Nov. 28, 11:59pm

1. Describe a method for protecting users against URL obfuscation attacks.

A user can enable a firewall onto their computer. Firewalls can prevent users from clicking on unauthorized websites through monitoring and filtering network traffic based on its ruleset. Implementing firewalls can protect users against URL obfuscation attacks while keeping their browsing experience safe.

2. Suppose a web client and web server for a popular shopping website have performed a key exchange so that they are now sharing a secret session key. Describe a secure method for the web client to navigate various shopping site pages, optionally placing things into a shopping cart. Your solution is allowed to use one-way hash functions and pseudo-random number generators, but it cannot use HTTPS, so it does not need to achieve confidentiality. In any case, your solution should be resistant to HTTP session hijacking even from someone who can sniff all the packets.

Let a user browse through the website. The browser will send a list of cryptographic ciphers and hash functions to the web server. The server then chooses the strongest cipher and hash function combination and sends this back to the web browser. This certificate will include the server's public key, allowing the browser to verify the authenticity of the server. The browser generates a random number, and encrypts that number with the server's public key, sending this to the server. The browser and server are then able to generate a shared secret key starting from the random number. The user's session will be saved via encrypting their inputs in their shopping carts with a key, which is then implemented into an optimal hash function.

3. What is the encryption of the following string using the Caesar cipher: INFORMATIONSECURITY?

Caesar Cipher: shifts letter by 3

A → D C → F
B → E D → G ... and so on.

Using Caesar Cipher to encrypt given string,
INFORMATIONSECURITY → LQIRUPDWLRQVHFXULWB

4. a. Compute the multiplicative inverse of 7 in Z23.
b. Show the steps and intermediate results of applying the extended Euclidean algorithm to compute the GCD of 512 and 240.

a) Inverse of 7 in Z23 is 2^7 or 2^7.

Using Euclidean,
23 = 7(3) + 2 gcd(23, 7) = 1
7 = 7(1) + 0
2 = 2(1) + 0

Using Euclidean backwards,
1 = 2 - 1(1)
1 = 2 - 1(27 - 7)
1 = 2(-14) + 13
1 = (2)(7) + (7) - 22

Inverse of 7 = 2^7

b) GCD of 512 and 240 is 16.
Using Euclidean,
512 = 240(2) + 32
240 = 32(7) + 16
32 = 16(2) + 0

gcd(512, 240) = 16

5. Find keys d and e for the RSA cryptosystem with p = 17 and q = 11; encrypt a given message M=88; show your steps. (Tips: you may use the following site is helpful in the calculation: https://www.wolframalpha.com/input/?i=19%5E5+mod+119)

given: p = 17; q = 11; M = 88

n = p * q = 17 * 11 = 187
ø(n) = (p - 1)(q - 1) = (17 - 1)(11 - 1)
= (16)(10)
= 160

public key e = integer & gcd(e, ø(n)) = 1 & 1 < e < ø(n)
let e = 7

finding private key d:
d = e^-1 mod (ø(n))
d * e = 1 mod (160)
d = 23

encrypt message through M^e mod n; this gives encrypted message cipher text c
c = M^e mod n
= 88^7 mod 187
88 mod 187 = 88

88^2 mod 187 = 7744 mod 187 = 77
88^4 mod 187 = (88^2 mod 187)^2 = 77^2 mod 187 = 5929 mod 187 = 132

88^7 mod 187 = (88^4 mod 187) * (88^2 mod 187) * (88^1 mod 187)
= ((132) * (77) * (88)) mod 187
= 894432 mod 187
= 11

Message M = 88 is encrypted as 11.

6. Demonstrate that the hash function H(x) = 5x + 11 mod 19 is not weakly collision resistant, for H(4).

In order to determine if a hash function is weakly collision resistant or not, we need to find some y such that $x \neq y$ and H(x) = H(y).

Let x = 4 and let y = 23;
H(4) = (5 (4) + 11) mod 19 = 31 mod 19
= 12

H(23) = (5(23) + 11) mod 19 = (115 + 11) mod 19
= 126 mod 19
= 12

Therefore, H(x) is not weakly collision resistant.

7. Explain why nonforgeability and nonmutability imply nonrepudiation for digital signatures.

Non-forgeability and non-mutability implies non-repudiation for digital signatures by providing validity for the origin and integrity of data. An individual can generate a signature that can be easily verified through readily available public information. This makes it impossible for an attacker to forge an identical signature of the individual from scratch.

8. Alice wants to send a large document as an encrypted attachment to an email to Bob over the internet. Alice also wants Bob to know that this attachment was sent by her (and not a forged attachment sent by someone else). Assume Alice and Bob have each other's public keys.
In the questions below, use the cryptographic primitives we've discussed in class. Define any cryptographic functions that you use. For example: one could say: - H is cryptographic hash function, or H is MD5;
- PKa, SKa, PKb, SKb Alice and Bob's public/private key pairs
- Ek()/Dk() Authenticated encryption/decryption scheme using key k (say, AESGCM)
- Enc()/Dec() Public key encryption/Decryption (say, RSA encryption)

- Sign/Verify Digital signature/verification algorithm (say, RSA signature)
a. Give the steps for Alice to prepare the attachment that will be sent.
b. Give the steps for Bob to decrypt Alice's attachment and verify that the message is valid and authentic (it has not been tampered and it was definitely sent by Alice).

a) Alice needs to pick a random, one-time symmetric key and use it to encrypt her attachment file. She then needs to encrypt the key with Bob's public key. She will need to digitally sign the ciphertext with her own private key.

k = randomKey() → c1 = Ek(M)

c2 = Enc(PKb, k) → sign = Sign(SKa, c1, c2)

Send: c1, c2, sign

b) Bob needs to verify the digital signature from using Alice's public key. He can then decrypt the symmetric key with his private key in order to decrypt Alice's attachment file.

if Verify(PKa; sign; c1, c2) = FALSE:
{ return ERROR }

k' = Dec(SKb, c2) → M' = Dk'(c1)
if M' = ERROR:
{ return ERROR }
else: return M'

9. Bitcoin is designed such that the attacker cannot reverse or tamper with the transactions. Explain how, referencing its technical design features as needed.

The network revolving around BitCoin uses cryptographic hashes to have proof of work through block chains. This allows for transactions to be validated while preventing double-spending. As new transactions happen within the BitCoin network, each node collects these transactions into blocks, and this uses the hash of the accepted block as the previous hash. As more blocks become accepted, the longer the chain becomes. This makes reverting or modifying transactions difficult due to the increasing number of blocks a chain might have.

10. a. Describe the difference between privacy and confidentiality.
b. In Cyber Forensics, it is important to acquire the evidence without altering the original. Name an approach to allow us to demonstrate that the image evidence is a true, unaltered copy of the original?

a) Privacy is the protection of an individual's personal information; it's the rights and obligations of individuals & organizations with respect to the collection, use,

retention, disclosure, and disposal of data. Confidentiality is the avoidance of unauthorized disclosure of information, involving the protection of data by allowing access for those who are allowed to see it while disallowing others from learning anything about its content.

b) Hash values, such as MD5 and SHA-1, can be used to demonstrate the image evidence as a true, unaltered copy of the original. When creating a new file or modifying an existing one, a new hash value will be generated. One can confirm if the file has been edited or changed by checking if the current hash value is matching the original file's hash value.