Quiz 6 student name: Evan Smith

1: 10 what’s the difference between Public key and Symmetric key? Why do we need public key method? Public keys encryption is asymmetric, that is, there is a public and private key (one for encryption, one for decryption). Symmetric key, as the name implies, uses the same key for encrypt and decrypt. The public key method is required because sharing a single key for all users of a site is impractical and doesn’t actually provide meaningful security, especially for public sites.

2: 5 what did those guys do to contribution greatly to public keys invention?

The RSA algorithm was invented by Ron Rivest, Adi Shamir, and Leonard Adleman. The dependence on primes to generate keys was critical for creating secure encryptions.

3: (15) What is Diffie\_Hellman Key Exchange (math formula)? How to explain it in a public key exchange? (which can be consider public key, which can be consider private key)

The Diffie-Hellman Key Exchange is achieved by agreeing on the public keys p and g. The sender then selects a secret integer a, and then sends the value A such that A = g^a mod p. The receiver does the same with their own secret. Finally, both sides can figure out the shared key s by computing s = B^a mod p or s = A^b mod p. After this s is the private key.

4: (15) what is the real public key exchange? How does it work? (no detail in math part, but with formula)

The common public key exchange is using PKIs to enforce that users apply to a CA for a certificate, which is then used to identify sites to users.

5: 25 what is man-in-the-middle attack? (explain it in a little tech detail, such as describe which key is used to do this attack and why it can be succeed).

The man-in-the-middle attack for encryption is when a third party intercepts a request by a user for a server’s public key. The attacker sends their own key instead, such that the response by the user can be decrypted by the attacker. It can then be sent along to the intended server using its public key. This means that it can succeed because the user would not easily see that their communications are being intercepted, since the traffic makes it to the destination successfully.

6: 15 how to defend the man-in-the-middle attack? How does it work? Which lab section is designed for it? (You can use our lab to describe how the defense work)?

One defense for MITM attacks is to assess the latency in the communication. This can be achieved by maintaining a log of the average connection time between two hosts, which is especially effective if there is consistent communication over a long time. Extended communication time can be indicative of malicious rerouting and a potential MITM attack.

7: 15 what is the disadvantage of public key? What is it used mostly for what encryption? Why?

The main disadvantage of public key encryption is that it is relatively slow. For that reason, it is often used for encrypting a shared, symmetric key which is then used to encrypt and decrypt the actual payload much more quickly.