Quiz 6 student name: Kevin Martin

1: 10 what's the difference between Public key and Symmetric key? Why do we need public key method?

A public key is a form of asymmetrical encryption that also requires a private key to work. A symmetric key is a single key that needs to be shared between the people who intend to send and receive the message.

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

James Ellis first conceptualized the public key/private key exchange.

Diffie and Hellman put the idea of a key exchange into practice, but failed to incorporate a private key decryption method.

Rivest, Shamir, and Adleman developed the RSA algorithm, which does incorporate a public key encryption and private key decryption.

Cocks devloped a near-identical algorithm in 1973 (three years before RSA) but was unable to disclose it until many years later.

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 a discrete logarithm: g^x *mod* P = b. If g, p, and b, but not x, it is a difficult problem to solved (no efficient algorithm).

The public key is g and p, with some information about x (but not x). The private key is x (for the sender) and y (for the receiver). Thus, both the sender and receiver generate a common number between themselves, the key, which is g^{x*y} *mod* p.

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

The real public key is g^x *mod* P, g, and p. It works because this is broadcast to everyone, and the receiver broadcasts back g^y *mod* P, g, and p, and only the original sender can decrypt it.

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 is when the attacker intercepts the sender's key and spoofs the public key, saying it's from the original sender. The key is e and n, so the attacker sends e' and n'. The receiver encrypts the message back using pk', and sends it back to the receiver. Now, the attacker can decrypt it and forwards a (newly) encrypted message back to the sender, saying it's from the receiver. Now the sender can decrypt this new message. This continues as long as the attacker is spoofing both the sender and receiver messages and encryptions.

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)?

To defend against the main-in-the-middle attack, you can use a digital signature.

It works by applying a “seal” to the message that **cannot** be forged by the attacker. These are created by algorithms. In the case of RSA, the signature is now M^d *mod* n, and only the sender can verify because e (public key) is public but b is private to the sender.

This is applied in Task 5 of the lab, which shows how a PKI can defeat the man-in-the-middle attack .

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

The disadvantage of the public key is that it is very expensive. The public encryption algorithm is 100x more expensive than symmetric key encryption.

It is mostly used for the initial key exchange. This establishes a session key, which allows the client and the server to switch to a symettric key encryption algorithm which is much vaster. This is done via the TSL/SSL protocol.