**HOMEWORK -5**

**1. Describe the Diffie-Hellman protocol.**

Diffie-Hellman key exchange is a method of exchanging cryptographic keys over a public channel securely. Diffie-Hellman protocol isa method for 2 computer users to generate a shared private key with which they can then exchange information across an insecure channel.

Alice and Bob are the 2 users. They agree on using 2 prime numbers g and p, where p is typically 512 bits and g is a primitive root modulo p. The numbers g and p need not be kept a secret from other users.

Say, Alice choose a large random number a as her private key and Bob chooses a large number b.

Alice computes A = g^a(mod p), which is sent to Bob.

Bob computes B = g^b(mod p), which is sent to Alice.

Now both, Alice and Bob compute their shared key.

Alice computes as K = B^a (mod p) = (g^b)^a (mod p).

Bob computes as K = A^b (mod p) = (g^a)^b(mod p).

Alice and Bob can now use their shared key K to exchange information without worrying about other users obtaining this information.

**2. Show how Mallory can conduct a man-in-the-middle attack when Alice and Bob perform the DH protocol from question #1.**

Say, Alice sends her public key to Bob. Mallory can intercept the key and send a forged message to Bob using Mallory’s public key. Bob receives this key, and assumes it’s Alice’s, and encrypts his message using Mallory’s key. When Mallory receives this message, the message is easily deciphered using his private key. He then encrypts the message using the public key from Alice and sends it to her. At this point, Mallory can easily alter the message and then send it to Alice. Alice would assume that the message came from Bob. This is known as the man-in-the middle attack.

**3. What is the recommended key size for p?**

512 bits. (wiki)

**4. Why is the recommended size for p for DH so much larger than the recommended key size for AES?**

**(search external sources for answering the last two questions, and cite your source)**

A 128-bit symmetric key is a bit more secure than a 2,048-bit asymmetric key. Symmetric simply means that the same key is used to encipher and decipher the encrypted web traffic. It's just any value of the right number of bits. The only way to break into a connection secured with a symmetric cipher is to try out all the keys. A 128-bit key means there are 340,282,366,920,938,463,463,374,607,431,768,211,456 possible keys to try.

A 256-bit key has the square of that many keys to try: a huge number. So, breaking 128-bit keys by brute force just isn't practical. And breaking 256-bit is even less possible. So, for symmetric ciphers, keys of these lengths make sense.

Asymmetric cryptography works by having two different keys, one for encryption and one for decryption. It's also often called 'public key cryptography' because it's possible to make one key public (allowing someone to encrypt a message) while keeping the other private (only the holder of the private key can decrypt the message encrypted with its related public key).Just as in the symmetric key case, attacks on say 2,048-bit RSA are based on trying out all keys of a certain size, but unlike the symmetric key scheme not every 2,048-bit number is an RSA key (because it has to be the product of two primes). So, although the key size is larger there are actually fewer possible RSA keys for any given number of bits that there are for the same symmetric key size. That's because there are only so many prime numbers of that size and below. The RSA scheme can only use pairs of prime numbers, whereas the symmetric schemes can use any number at all of the same size. If you used a 256-bit RSA key (roughly consisting of two 128-bit prime numbers multiplied together) you'd quickly find that your encryption had been broken by someone using a fast home PC. There are only so many 128-bit prime numbers and there are fast ways of attacking the factorization problem (such as the General Number Field Sieve that actually make breaking RSA keys a little easier than trying out every single key).

So, asymmetric keys have to be much larger than symmetric keys because there are less of them for a given number of bits, and because there are patterns within the keys themselves.

Source: https://blog.cloudflare.com/why-are-some-keys-small/