Deniz Aytemiz

ECE 5560-Assignment 4

Question 1: Multiple Choice:

1. C
2. B
3. D
4. D
5. B

Question 2: Encryption & Random Number Generation

1. Just like symmetric, asymmetric encryption schemes are also vulnerable to a brute force attack. One can try every possible key for the scheme. For avoiding these attacks large keys must be used. However it should not be very large such that it makes the encryption and decryption process impractical.

   Another attack is mathematical attack. Attackers can try to find the private key from the public key. For example for RSA, if your public key size is too short, factoring it with brute force will not be hard to do. One can factorize 256 bit modulus in a couple of minutes with brute force.

   There are timing attacks too that can work on any public key cryptography. In timing attacks the attacker observes the running time of a cryptographic algorithm and thereby tries to deduce the secret parameter involved in the operations. For a timing attack on RSA for instance, the attacker needs to have the target system compute C^d mod N for multiple selected values of C. By measuring the amount of time required and analyzing the timing variations, the attacker can recover the private key d one bit at a time until the entire exponent is known.

   There is a fault-based attack targeted towards RSA. The attacker attacks the processor and causes faults in the signature computation. These false signatures can later be analyzed by the attacker to find out the private key.

   There is also the chosen ciphertext attack. The attacker can exploit the properties of RSA by choosing multiple ciphertexts and getting corresponding plaintexts, the attacker is able to select blocks of data processed using private key yielding information needed for cryptanalysis.

2. Hard to solve mathematical problems is what modern cryptography makes use of to create really hard to break schemes. It is assumed that if the problem is hard enough there will be no efficient algorithm that can solve it. For instance factorizing the modulus to its prime components is a hard problem that lies in the heart of RSA.Even though these hard mathematical problems make it difficult to break/attack a scheme it is not impossible to attack anyways. One can find private keys in RSA by factoring if the key size is too small

for instance. So one cannot say that hard problems make cryptographic schemes 100% secure.

3. DH is one of the earliest practical examples of public key exchange. It is useful since it allows two parties to communicate over an unsafe channel and come up with a shared secret that they can use to make encryption keys for their communications. It does not matter if someone is eavesdropping since the complete secret is not sent over connection. The scheme is resistant against brute force attacks since it is infeasible to try all options but it can be attacked with man in the middle.