Computer Security   Homework 4 (Due Friday 9/11/20)

1. True or False.

   (a) Trying all possible keys systematically until one works is a typical side-channel attack for breaking cryptography.

   (b) Probing the CPU's cache for remnants of the encryption key is a typical side-channel attack for breaking cryptography.

   (c) Using the sounds emitted by your CPU is a typical side-channel attack for breaking cryptography.

   (d) Primes that are 100 digits long are typically considered safe to use for Diffie-Hellman.

   (e) AES is a type of public-key cryptography.

   (f) Diffie-Hellman should be combined with an authentication scheme and not used alone.

   (g) RSA is considerably faster for encrypting data than AES.

   (h) RSA is one of the most dependable encryption algorithms, with very few known attacks on it.

   (i) Multiplication of prime numbers/factoring is the trapdoor function behind RSA.

   (j) The problem with the string comparison algorithm we looked at in class is that the comparison takes differing amounts of times depending on the user's string, allowing them to work out what the secret string is.

2. Alice and Bob use Diffie-Hellman to generate a shared secret. They then use that shared secret to

   (a) verify that each is who they claim to be

   (b) determine which type of encryption to use

   (c) create encryption keys to use with AES or some other symmetric cipher

   (d) create a public/private key pair

3. Suppose Alice chooses a random number, encrypts it with her private key and sends the result to Bob. Bob then decrypts the random number with Alice's public key. This is an alternative to what process we covered in class?

4. Alice and Bob do a Diffie-Hellman key exchange. They use the prime $p = 17393$ and generator $g = 3$. Alice chooses the random number $a = 101$ and Bob chooses the random number $b = 4522$. Remember that python can do $g^x \bmod p$ via `pow(g,x,p)`.

   (a) What are the values that Alice and Bob send to each other?

   (b) What is the shared secret value that Alice and Bob both compute? Show the calculation that each does to get it.

5. Suppose Alice chooses $p = 179$ and $q = 223$. She then chooses $e = 5$ and computes $d = 31613$. This is all for RSA.

   (a) What values will Alice publish as her public key? Give the exact numerical values.

   (b) What will she use as her private key? Give the exact numerical value.

   (c) Suppose Bob wants to encrypt the message 250. What is the encrypted value of 250?

   (d) Show the computation that Alice does to decrypt Bob's message. Make sure you get 250 as the answer.

6. Suppose Alice and Bob are performing a Diffie-Hellman key exchange. They agree to use $p = 287137$ and $g = 10$. Eve, the eavesdropper, sees these values, and she sees Alice send 33002 and Bob send 202474. Because Alice and Bob are using such a small prime, it is possible for Eve to figure out the shared secret by a brute-force search. What is that shared secret? Include any code you use to solve the problem.