Week 9 Questions

**Lecture 46**

1. subBytes and mixColumns replace the values with new values so they are not recognizable.
2. ShiftRows uses diffusion by shifting the bytes so that they are not the same.
3. Inverting the MixColumns requires multiplying each column with a fixed array therefore it takes longer than encryption.
4. Each round would further change the values so that it is not recognizable. Therefore by increasing the number of rounds, the values are less recognizable.

**Lecture 47**

1. If you have identical blocks in the plaintext, then you would have identical blocks in the ciphertext. You could still decipher the ciphertext because of the clues given.
2. You can fix this flaw by using CBC.
3. If an attack can observe changes to the ciphertext, then he may be able to see the first block changed. Also, if the attack can find two identical blocks, he may be able to derive the relationship used in CBC.
4. Standard block encryption modes encrypts messages but they are still recoverable. However, key stream generation uses a pseudorandom number generator and is used once.

**Lecture 48**

1. The private key.
2. It is important for public key systems because if the function was easy to invert, the it would be easy to find the private key from the public key.
3. The public key is available for everyone to use but is still unique to each person. You no longer have to find a way to keep a shared secret secure.
4. $\{P\}K^{-1}$
5. Symmetric algorithms are more efficient and use efficient machine operations like bitwise operations, whereas asymmetric requires things like factoring. A public key encryption (an asymmetric algorithm) may take 10,000 times longer to perform than a symmetric encryption.

**Lecture 49**

1. Yes, because the RSA algorithm implements the use of encryption and decryption keys symmetrically.
2. RSA uses prime numbers because the product of two prime numbers are hard to factor.
3. Yes
4. They don't have A's private key to decrypt the message.
5. There isn't a key that would identify that the message originated from B.
6. A is sure the message came from B because B's private key is used to encrypt the message and only B's public key would decrypt it.
7. Everyone has B's public key so anyone can decrypt the message.
8. B can encrypt with it's private key then with A's public key. This would ensure that only A can decrypt and that the message came from B.

**Lecture 50**

1. So you can hash inputs quickly.

2. For weak collision resistance, given one input, it is hard to find another input that does not equal the given message. For strong collision resistance, it is hard to find two inputs that would make the function outputs equal.
3. Preimage resistant, if given h, it is hard to find a message where h = f(m). Whereas, second preimage resistant, it is hard to find to find an input that does not match the given input.
4. 1.25*2^64 values before finding a collision
5. 1.25*2^90 values before finding a collision
6. Cryptographic hash functions are used to ensure that the value received is the same as the value sent; if the file is tampered with then the hash values would not be the same. If you used them for confidentiality, all messages from a person would hash to the same value.
7. A cryptographic hash function "binds" the bytes of a file together so that any alterations to the file are apparent.
8. B can encrypt the message by using a cryptographic hash function on the message, then encrypt the message with it's private key. Then encrypt the message with A's public key.

**Lecture 51**

1. No, because S does not know R's private key.
2. Yes, you can but it may not ensure authenticity. Someone could come along and change the outer encryption to his/her own private key.
3. No.
4. Key exchange requires confidentiality and authentication because you don't want anyone else know the message you're trying to send but also don't want someone else pretending to be you sending the message.

**Lecture 52**

1. It would still take the eavesdropper forever to figure out the shared secret.
2. Attacker may be able to find out B.
3. Attacker may be able to find out A.