Chad Custodio
Cgc735
Aitan791
chadcus@gmail.com

Week 3 Questions

Lecture 34
1. Because whatever you encode should be close to entropy, but never better than it.
2. If you keep trying to push through the message, then it will eventually break through the noisy channel.

Lecture 35
1. -(log(1/10))
2. There are so many factors that go into figuring out the entropy because of how the different conventions are.
3. Zero assumes that all elements have equal probability of coming out. First has predicted probabilities. Second and Third basically predicts a certain common sequence in the code.

Lecture 36
1. Because certain senarios don't have obvious predicted outcomes.
2. Because depending on the observer's position, they will know more than somebody else that has to guess the result of something, making it easier to compute.
3. The better the coding/entropy, the less redundancy there is.

Lecture 37
1. Context can help decipher what the person is trying to convey in a certain language. Symbols can also help with getting to know more about the context. Would there be any sort of transformations that could encrypt it more.
2. The encryption algorithm is enough to create a ciphertext but a key can help make the encryption better.
3. It should be preserved
4. May mean regularities, which an attacker can use to break through the encryption

Lecture 38
1. D(E(P))
2. D(E(P,Ke),Kd)
3. It gives some clues about the certain senario
4. Knowing frequency of letters helps find certain patterns of what might be said

Lecture 39
1. Because it could take forever to actually find what you are looking for. Even then, you need a way to figure that out.
2. When you are searching a linear space, you should find it halfway down. This means you cut the operation by half which explains the n-1.

3. When put together, it makes it harder to figure out what the message is because not only are you replacing symbols, you are also rearranging them so that there is less of a pattern to be found.
4. Confusion is more about to making it the information harder to understand whereas diffusion is about spreading out the information by moving it around
5. Encryption

Lecture 40
1. Monoalphabetic replaces symbols with the same substitution symbol throughout whereas polyalphabetic uses different symbols.
2. However you specify the mapping.
3. Since you use the same key symbol, there is no variation to make the mapping any more complicated
4. However many spaces you shift
5. 25/26
6. No
7. Find ciphertext symbol, which is in the map, and the key symbol, the column of the map, to find the appropriate row.

Lecture 41
1. Assuming it is not simple, there are 26 letters and you are trying to find 3 specific letters. Making it 26 to the power of 3.
2. Receiver now knows that it is a simple solution.
3. Yes because there could be a more complicated way of finding out the plain text that isn't given in the algorithm or ciphertext.

Lecture 42
1. Any possible plaintext could be the pre-image of the ciphertext and because the key is random, the plaintext could be any possibility of that length.
2. If given any knowledge about the key, you could potentially narrow down the possible plaintext.
3. If there is a secure channel to send the key, then there is no reason to have one. But if there isn't one, then there is no way to distribute the key in a secret manner.

Lecture 43
1. It preserves the symbols of a text and it doesn't take into account digrams and trigrams.

Lecture 44
1. symmetric
2. Key distribution is about having secure transportation of the key where as key management is making sure that keys preserve their own safty and making them available when needed.
3. No because you would need the private key.
4. Symmetric encryption system it is easier to generate and it is random.

Lecture 45
1. Because you encrypt a whole group of text rather than one symbol directly.

2. You don't want things to be malleable because it could change something in the plaintext.
3. You can chain together services without exposing any of the data.

Lecture 46
1. subBytes- replace byte by a value stored at that value index in a table
addRoundKey- XOR the state with a 128-bit round key derived from the original key
2. shiftRows- shift rows by a certain amount of bytes depending on location
mixColumns- replace column by its value multiplied by a fixed 4x4 matrix of integers.
3. In mixColumn, you have to multiply by the inverse. This isn't as optimized as it was in encryption.
4. Makes things more useful by grouping up bits and then moving/replacing them with the rounds.
5. You need more rounds for higher amount of bits.

Lecture 47
1. Identical blocks in the plaintext yield identical blocks in the ciphertext.
2. Randomize the blocks before they are encrypted.
3. Observed changes and content leak.
4. It is used more as a pseudorandom number generator.

Lecture 48
1. A secret key.
2. Because it becomes hard to invert without additional information.
3. Because you can give the public key and it doesn't matter if it seen or not because the sender is the only one that can decrypt with it.
4. {{{P}K}K-1}K
5. Asymmetric algorithms are much less efficient.

Lecture 49
1. Yes because you can use either key for decryption or encryption.
2. It is easy to multiply two primes
3. Yes
4. Because A is the only one that should be albe to decrypt the message.

Lecture 50
1. To make things easier when trying to find matching hash values
2. Weak collision means it is hard to find a message that matches anothers hash value while strong resistance means it is hard to find two messages with the same value.
3. Preimage you are given a hash value and need to find the a message that matches the value. Second preimage is about finding another messages with the same hash value.
4. 1.25 times 2 to the power of 64 to find the collision.
5. 1.25 times 2 to the power of 80 to find the collision.
6. Because we are more concerned about making sure that nothing in the message has changed.
7. Compute the hash function, everytimes the file is used or accessed, recompute the hash. Then compare it to the stored value.
8. It will append the hash to the end of the plaintext and encrypt that after the RSA.

Lecture 51
1. No because you don't know if it was sent securely because the R private key was sent.
2. Yes because you will still know who sent it and the receiver's private key will strip off the public key
3. Yes
4. You need two levels of encryption because you want both confidentiality and authentication.

Lecture 52
1. Eavesdropper will not get anything.
2. Nothing because they would still need b
3. They still wouldn't be able to figure out the shared secret number.