Name: Tolu Kalejaiye
UTEID: tok76
CSLogin: tok76

Homework 3

Lecture 34

1. That would exceed the capacity of the channel.
2. It removes unnecessary data, allowing for only the important information to be transmitted, since some of the capacity of the channel is taken up by noise.

Lecture 35

1. 2.302
2. The probabilities of each letter occurring are not equally likely and letters are not independent of each other. Thus, more complex models are required.
3. They have to do with the independence/non-independence of symbols to one another with zero being independence, and third order being trigrams.

Lecture 36

1. The information content may be large depending on how much knowledge you have of the message. That makes it harder to predict the probability, especially in real world situations where all outcomes are not equally likely.
2. If you were the person who wrote the message initially, you know what it is and have no uncertainty. If you have no knowledge, then it's harder for you to figure out what it says, and makes the information content larger.
3. The more redundancy, the less entropy.

Lecture 37

1. It's a numeric encryption so each number could possibly stand for something, with the special characters denoting where a particular sequence of symbols may end or begin.
2. This may depend on the type of encryption you choose to use. If it's simple enough, you may not need to apply a key to it to decode the message. For example, a simple letter number substitution wouldn't need it.
3. It increases it.
4. If you can figure out what the redundancy represents, you can use that to figure out a large part of the message if the message contains a lot of redundancy.

Lecture 38

1. D(C)

2. $\{\{\{\{P\}_{Ke}\}_{Ke}\}_{Kd}$
3. To make it easier to decipher future messages. The same patterns could be used in other encryptions.
4. They could tell the cryptanalyst certain things about the syntax of the language that could make the message easier to interpret.

Lecture 39

1. Though it's breakable, the only way to break it might be the brute force approach, which may take a very long time.
2. ?
3. They're good at confusion and diffusion, which are important in encryption.
4. Confusion leaves the information where it is, but makes it look different. Diffusion moves symbols around.
5. Used together, they're equally good for encryption. Diffusion may be the harder one to crack though.

Lecture 40

1. Monoalphabetic substitution is uniform, polyalphabetic substitution makes multiple substitutions.
2. The key would be a mapping of the symbols to their corresponding encrypted symbols.
3. Because for each letter, there are k-1 possible substitutes for it.
4. The key would be each letter corresponding to another letter two letters away.
5. 26
6. No, it isn't
7. It would be the inverse of the encryption algorithm

Lecture 41

1. Because for each letter, there are 26 possible letters it could represent, thus 26^3.
2. Since we know it's a simple substitution, then we just multiply the number of symbols by the number of symbols in the key.
3. No. If not knowing the encryption algorithm doesn't lessen the search space, the cipher would be too complex to be realistic.

Lecture 42

1. Because every possible plaintext could be the pre-image of that ciphertext under a plausible key.
2. Because then a pattern can be determined.

3. The key distribution problem is simply about how to transfer the key/whether it's even necessary or not. If you can't securely transfer the key, then it becomes useless because it can be intercepted.

Lecture 43

1. Letter frequencies are preserved as well as the actual symbols, thereby making the message easier to decode.

Lecture 44

1. Asymmetric
2. Key distribution is about transporting a key, key management is about dealing with all the keys you have.
3. Not if it's asymmetric. That would require having the private key that the receiver of S's messages holds.
4. They can both be strong or weak, but symmetric encryptions are easier to generate.

Lecture 45

1. Because they offer a high level of diffusion that makes them harder to break.
2. It makes an encryption less secure.

Lecture 46

1. Subbytes. Replaces bytes with values stored in a 256 element lookup table.
2. ShiftRows. Shifts symbols left depending on where they occur.
3. Because the mixColumns step requires multiplying by bigger numbers than in the encryption step.
4. The blocks are the amount of info we're encoding at one time, and the rounds are the steps used to encode the blocks.
5. Either to achieve greater encryption, or to allow for encryption of a larger number of bits.

Lecture 47

1. The blocks are in order and so knowledge of the plaintext/ciphertext can give you knowledge of the ciphertext/plaintext.
2. By using CBC.
3. Content leak and observed changes.
4. EBC and CBC aim to store the message in an encrypted fashion whereas key stream creates a key stream that you can use to decipher the message.

Lecture 48

1. The secret key

2. So that it can't be inverted and used to decrypt the message.
3. By using a secret key that isn't distributed, even if the public key is intercepted, you can't do anything with it because it won't work without the private key.
4. $\{P\}_{k-1}$
5. Asymmetric algorithms are generally much less efficient than symmetric algorithms.

Lecture 49

1. Yes. $\{\{P\}_D\}_E = P = \{\{P\}_E\}_D\}$
2. Since we mod $(P^e)^d$ by n to get P, $(P^e)^d$ would probably have to be a prime number, otherwise we'd get a 0 every time for P.
3. Yes.
4. They would need the private key.
5. Someone could have intercepted the message and then sent it to A.
6. Because it was sent with B's private key.
7. Because all the person would need is B's public key which is easier to access.
8. Include another pair of keys for authentication.

Lecture 50

1. To avoid large overhead.
2. Strong collision has to do with the values not matching after applying the function, and weak collision has to do with them not matching before the function is applied.
3. A function f is preimage resistant if, given h, it is hard to find any m such that h = f (m). A function f is second preimage resistant if, given an input m1, it is hard to find m2=m1 such that f(m1) = f(m2). This is sometimes called weak collision resistance.
4. 1.25*sqrt(128) different arguments.
5. 1.25*sqrt(160) different arguments.
6. Because they're used for integrity
7. "Sealing" the file

Lecture 51

1. Yes.
2. No.
3. Yes.
4. Confidentiality and authentication.

Lecture 52

1. Nothing. The eavesdropper doesn't know b.
2. Nothing because the eavesdropper doesn't know a.

3. Nothing because the eavesdropper doesn't know b.