Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

Week 3 Questions

Lecture 34

1. It is impossible to have a better rate than C/h because C/h is the absolute perfect encoding of the entropy.
2. Increasing the redundancy over a noisy channel can allow a message to get through the channel because the message will get through after an arbitrary amount of tries.

Lecture 35

1. H = -(log(1/10))
2. A reason is that there are instances that other letters or symbols are more frequent than other letters and symbols. This causes the entropy to be not completely true.
3. Zero-order is the equal chance of any letter being picked. First-order involves the probability of a single letter being picked based off of the language. Second-order is the likelihood of two concurrent letters or symbols being chosen and third-order is the same as second-order except for it is three consecutive letters or symbols.

Lecture 36

1. Circumstances can prove the prior possibilities to be completely different in all instances.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

2. Based on who the observer is, the message relative to the knowledge of that observer can differ in entropy to the other observers.
3. Entropy can be used to determine the redundancy in the encoding.

Lecture 37

1. The encrypted message only uses the numbers 0-9 and the symbols *, +, :, ;, (,), +, and !. These symbols and numbers could relate with a key on how to decipher the code.
2. There wouldn't be any use for a key if the decryption was just writing the document back words and not substituting letters for other symbols or letters.
3. Encrypting a text can render the text to be unreadable or not useful for any eavesdroppers accessing the file.
4. Redundancy is a big enemy because the eavesdropper can find similarities and patterns created by the encryption process to decrypt the file.

Lecture 38

1. $P = D(E(D(E(P))))$
2. $E(P, K_E) = D(E(E(P,K_E),K_E),K_D)$
3. Finding patterns and repetition of certain symbols can help them break an algorithm.
4. Patterns within letters used in a language can be helpful for the analyst.

Lecture 39

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

1. It may not be feasible to break because the only way to break it is through brute-force and that could take a lot of time.
2. Because on average, most plaintext/ciphertext are cracked at around half way through the available key.
3. Substitution and transposition are usually combined in most modern commercial symmetric ciphers for encryption and they have proved to be very useful.
4. Substitution tends to be good at confusion while transposition is good at diffusion.
5. Both are important because the combination of both maximizes the effects of the encryption.

Lecture 40

1. A monoalphabetic cipher uses a 1-1 mapping of symbols, and a polyalphabetic substitution substitutes symbols based on where the symbol occurs in the plaintext.
2. Whatever you decide what table to use for mapping each symbol to a designated character.
3. Depending on how many symbols there are, there can be k possibilities for each symbol to have but cannot be repeated in that mapping.
4. The example ciphertext designates the letter to be the letter two spaces ahead.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

5. 26
6. No
7. A polyalphabetic substitution

Lecture 41

1. Because each space has a possibility of 26 letters giving $26^3 = 17576$
2. Because y will have the same symbol and after the x is figured out there are 25 letters left to figure out the last two for y.
3. A perfect cipher is not possible because there is always going to be a way to breach the computer security to crack the cipher. I just believe there is a way to solve everything.

Lecture 42

1. Take an arbitrary key plain text that is the same length as the plaintext and XOR'd it with the plaintext only once.
2. If you knew something about the key, working backwards and knowing the pattern could make it possible to cut out half the keys based on the pattern.
3. The sender and receiver have to have a secure channel to transfer the key to decrypt the cipher.

Lecture 43

1. The cipher is not particularly strong because the symbols are rearranged but not substituted, and that leaves space for someone to have all the characters they need to decrypt the message.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

Lecture 44

1. Symmetric
2. Key distribution is who can have access to these keys and how to send them securely and key management is how to keep the abundance of keys secure from being accessed.
3. No they cannot because they do not have the private key.
4. Yes, because symmetric keys are easy to generate and are not as costly as public key systems.

Lecture 45

1. The block encryption makes it harder to decrypt based of the high diffusion and immunity to tampering and it is non-malleable.
2. Malleability allows an attacker to manipulate the ciphertext with predictable effects on plaintext.
3. Homomorphic encryption is a form of encryption where a specific algebraic operation performed on the plaintext is equivalent to another algebraic operation performed on the ciphertext.

Lecture 46

1. subBytes demonstrates confusion because they replace bytes by the value stored at that location.
2. shiftRows demonstrates diffusion by shifting the rows.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

3. It takes longer because the MixColumns step has to multiply by the inverse of the array and that is time consuming.
4. AES allows keys of size 128-bits, 192-bits, and 256-bits, with 10, 12, 14 rounds, respectively.
5. More rounds would suggest the number of byte blocks to access and solve the decryption.

Lecture 47

1. Identical plaintext blocks contain the same encrypted blocks
2. Use CBC
3. An attacker can observe ciphertext over time to spot the first block that changed and there can be a content leak that allows the attacker to drive information about the two plaintext blocks.
4. Bits appear random but they are actually not and it uses a one-time pad.

Lecture 48

1. The decryption key must be private.
2. It is easily computed and near impossible to decrypt without additional information.
3. The public key can be seen by anyone but the only person who can decrypt is the person with the private key.
4. $\{P\}_{K^{-1}}$

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

5. Symmetric encryption plays the workhorse of most modern commercial encryption while asymmetric encryption has a few vital roles in the process.

Lecture 49

1. The keys are used in a symmetric fashion, which allows both keys to be used for decryption and encryption.
2. The prime numbers create a difficulty in factoring the large numbers.
3. It is breakable.
4. Because the person is not sure who is sending the message and the key could be different.
5. A cannot be sure because they are not using B's public key for authenticity.
6. A knows that B has access to B's keys and knows that they are the sender.
7. They can save B's private key and find B's public key that is available and decrypt their message.
8. A must have access to B's private key and send A the encrypted message using his public key.

Lecture 50

1. Because there is a fixed finite amount of hash values.
2. A weak collision would be easy to find two messages that are equal, while strong collisions are based on the difficulty of finding two messages that are the same.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

3. A preimage is hard to find a value h based on the function f with message m. So it would be hard to find h = f(m). Second preimage is an example of a weak collision.
4. The set of hash numbers would include $1.25*2^{64}$
5. The set of hash numbers would include $1.25*2^{80}$
6. Document retrieval system containing legal records, it may be important to know that the copy retrieved is identical to that stored. Also, in a secure communication system, the correct transmission of messages may override confidentiality concerns.
7. It is tamper-resistant if computing the hash function of H(M) and then recomputing the file again. If H(M) is still the same after the recomputed, then the tamper-resistant conditions are met.
8. Yes because the RSA would ensure the confidentiality.

Lecture 51

1. No, because the confidentiality is breached using R's private key.
2. No, because the confidentiality would be breached using S's private key at the end to R's public key.
3. No, because R does not know S's private key, yet and cannot decrypt the final encryption.
4. Key exchange must ensure confidentiality and authentication.

Lecture 52

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

1. If they do not know b, they cannot find out anything based on the information they have.
2. Nothing would happen in this instance.
3. However, if b were to be discovered, the eavesdropper can find the value and crack the cipher.