Name: Olamide Fayemiwo
EID: oaf226
CSLogin: ofaye
Email: olamide.fayemiwo@live.com

Week 3

Lecture 34

1. It is impossible to transmit a signal over a channel at an average rate greater than C/h because it means that some encoding was compressed beyond the entropy in the language.
2. Increasing the redundancy of the coding scheme can increase the reliability of transmitting a message over a noisy channel by allowing the channel to be able to physically handle the message traffic so as to allow the channel to be able to transmit with arbitrarily small error rate.

Lecture 35

1. The entropy of the language is: h = -(log(1/10) = 3.32
2. Computing the entropy of a natural language is difficult because it contains significant redundancy, some letters follow other letters frequently and others not at all, it also requires complex models.
3. Zero-Order Model is when each character is statistically independent of all other characters and all are equally likely to occur; the First-Order Model is when each character is independent of one another but the probability distribution of the characters are according the distribution of the English text (their frequencies); Second-Order Model occurs when there are some dependencies between the characters, the characters close to each other are more dependent than those that are far away (It is also based on frequencies) and the Third-Order Model is when the present character depends on the previous two characters but it is conditionally independent of all previous characters before those.

Lecture 36

1. Prior probabilities are sometimes impossible to compute because the information content of a message depends on the state of knowledge of an observer.
2. The information content of a message is relative to the state knowledge of an observer because the receiver actually knows the content of the information so there is no uncertainty.
3. The relationship between entropy and redundancy is that entropy is the measure of uncertainty and it can be used to measure the amount of redundancy in an encoding. There is no redundancy in the encoding if the information content is equal to the length of the encoded message.

Lecture 37

1. There are a lot of redundancies in the encrypted message which means that if it were possible to figure out the redundant characters, it might be slightly easier to actually decrypt the message.
2. A key may be optional for the process of encryption or decryption due to the level of the information being passed. It relates to confidentiality and integrity, you want the information to be protected when encrypting it and you want to prevent certain writes to it when decrypting.
3. It makes it unreadable by people who do not have the key to decrypt it.

4. Redundancy in the source gives clues to the decoding process because figuring out which character represents which can make the process of decrypting easier and faster to an individual who is not authorized to see it.

Lecture 38

1. C = E(P) and P = D(C) and C1 = E(P) and P1 = D(C1)
2. This cannot be written to a simplest form because you cannot input a ciphertext into an encryption.
3. A cryptanalyst might want to recognize patterns in encrypted messages as a way to decrypt the message in an easier way and make it faster/ efficient to decrypt.
4. Properties of language might be of use to a cryptanalyst because it can make the process of identifying redundancies and patterns more efficient by using one of the orders (Zero, first, second and third order model). They can get the entropy of the message and calculate frequencies.

Lecture 39

1. An encryption algorithm may be breakable but not feasible to break because the analyst has to try multiple ways of decrypting the message and it has to be successful. It is challenging to figure out a solution easily to break it but it can be broken.
2. K can be recovered by exhaustive search in an expected time on the order of 2^(n-1) operations because it checks for all information in the plaintext and strong algorithms are hard to break.
3. Substitution and transposition are both important in ciphers because they can help scramble the message in order to protect the content of the information. It will make it difficult to decipher the content of the message because substitution replaces the character for another and transposition changes the order of the words. So for example, the order of the words may be backwards, or swap the characters if they are even and leave the middle character if the word is odd.
4. Confusion is a way of transforming information in plaintext so that an interceptor cannot readily extract it while diffusion is a way of spreading the information from a region of plaintext over the ciphertext.
5. I think diffusion is better for encryption because it makes it is already challenging to figure out what the text is actually saying and it takes it even more challenging figuring out the order it is supposed to be placed. If the message has been decrypted, it might still be difficult to figure out the exact content of the message due to diffusion.

Lecture 40

1. The difference between monoalphabetic and polyalphabetic substitution is that monoalphabetic substitution is done uniformly meaning it is done in order while polyalphabetic substitution is done depending on where the plaintext symbol occurs.
2. The key in a simple substitution cipher is the substitution letter (its position)
3. There are k! mappings from plaintext to ciphertext alphabets in simple substitution because it is a 1-1 mapping and in order to find what it entails you can find its permutation if you know how many characters there are. This simply means that if there are 3 characters it takes 3! [3 x 2 x 1] ways to break the code.
4. The key in the Caesar cipher example is the distance (shifts made) between the number and its replacement letter.
5. The size of the keyspace in the Caesar Cipher example is the number of alphabet 26.

6. The Caesar Cipher algorithm is not strong because there are only 26 keys being used and brute force can be used as a method to break the code.
7. The corresponding decryption algorithm is to subtract the key value at that position from the ciphertext value at the same position and mod it by the number of the alphabet 26.
   Plaintext = (Ciphertext - Key) % 26

Lecture 41

1. There are 17576 possible decryptions for the "xyy" encoding because it is using a substitution cipher which uses the English alphabet of 26 letters and there are 3 letters to permute. Therefore 26^3 are the possible decryptions for the encoding.
2. The search space is reduced by a factor of 27 because it states that it is using a simple substitution which substitutes English alphabet uniformly. Once a letter has been substituted for x, there is only 25 more alphabets to use where only one would be needed for the 'yy'. So 26 x 25 is the possible decryption.
3. A perfect cipher is possible by having multiple possible keys as plaintext, with the key chosen randomly.

Lecture 42

1. The one-time pad offers perfect encryption because the ciphertext does not provide information about the plaintext to anyone who is trying to break its encryption, and the key can only be used once.
2. It is important for the key in one-time pad to be random because it makes it hard to figure out the plaintext if the ciphertext is known.
3. The key distribution problem is figuring out how to share secret keys to establish secure communication in which a large number of parties must pairwise; it tends not to go well. It is challenging for the sender and receiver to decide on a secret key when the key is used only once.

Lecture 43

1. The downside to using encryption by transposition is that it is easy to decipher because it does not change the characters in the plaintext, it only reorders them.

Lecture 44

1. The one time pad is a symmetric algorithm because it uses the same key for both encryption and decryption but it can only be used once.
2. Key distribution is a problem of identifying how to convey keys to those who need them to establish secure communication while key management is how to preserve the safety of a large number of keys and making them available when needed.
3. If a person gets a hold of Ks it would be challenging to decrypt S's encrypted messages because a private key Ks^-1 is needed to decrypt the message which S holds. It is easy to get a hold of Ks because it is a public key, different keys are needed for encryption and decryption.
4. Public key systems are better because there needs to be a public key to encrypt and a private key to decrypt which is held by the subject. Symmetric encryption needs each pair of users to share a secret key.

Lecture 45

1. Most modern symmetric encryption algorithms are block ciphers because block ciphers can handle large amounts of data.

2. The significance of malleability is that it shows which cipher is stream or block structured. Block structured ciphers are not malleable because that means being able to make changes on the ciphertext which produces meaningful changes in the plaintext.
3. The significance of homomorphic encryption is that it converts data into ciphertext that can be analyzed and worked with as if it were still in its original form. (It does not compromise its encryption)

Lecture 46

1. subBytes uses confusion in AES because confusion is when you replace a character for another. In subByte,s for each byte in the array, it uses its value as an index into a 256-element lookup table, and replace byte by the value stored at that location in the table.
2. shiftRows uses diffusion in AES because diffusion is when you relocate certain characters (shifting it). For example: in shiftRow Let Ri denote the ith row in state, shift R0 in the state left 0 bytes, then shift R1 left 1 byte, then shift R2 left 2 bytes and then shift R3 left 3 bytes. This causes a shift in the array which changes the position of everything.
3. Decryption takes longer than encryption in AES because decryption involves inversing the encryption – one of the 4 steps of AES (mixColumns) is particularly hard to inverse because you have to multiply each column by a fixed array.
4. The use of the blocks in AES is to firstly secure encryption and decryption of the 128 bits and the rounds is the key size which specifies the number of repetitions of transformation that converts the plaintext to a ciphertext. It has several steps to take in order to encrypt messages.
5. One would want to increase the total number of Rounds in AES because you want to be able to handle large number of blocks (data) brought in.

Lecture 47

1. The disadvantage in using ECB mode is that it leaves too much regularity in the ciphertext
2. This flaw can be fixed by using a CBC (Cipher Block Chaining) which is randomizing the blocks before they are encrypted.
3. The potential weaknesses of CBC are that an attacker may be able to observe changes to the ciphertext over time and will be able to spot the first block that was changed and is the attacker finds a way to find two identical ciphertext blocks, and then he can derive information about plaintexts.
4. The key stream generation is different from the standard block encryption because the key stream generation uses the cipher as a pseudorandom number generator in which it returns a key stream that can be used as in one-time pad while block encryption generates the ciphertext that stores the message in encrypted but recoverable form.

Lecture 48

1. For public key systems, the private key for decryption must be kept secret in order to ensure secrecy.
2. One-way functions are critical to public key systems because it makes it difficult to invert the function without additional information.
3. Public key systems largely solve the key distribution problem by it having a way for encryption and decryptions communicating with each other (having a shared key) in which the key can be used in either function.
4. P = {{P}k}k-1

5. The asymmetric algorithm works on simple bit-wise operations which play some roles in cryptography while symmetric algorithm works on more complex operations and does more when it comes to commercial cryptography.

Lecture 49

1. Yes, the algorithm will still work if you switched the public and private keys in RSA because both keys can be used for encryption and decryption.
2. Prime numbers are generally easy to multiply together but it is challenging to factorize a given number into prime factors. This applies to RSA because it is easy to encrypt the file but in order to invert it to decrypt can be challenging.
3. RSA is breakable, depending on the number of bits.
4. No one interrupting {M}Ka can read the message because they do not hold the private key to decrypt it.
5. A cannot be sure that {M}Ka came from B because it could be an intercepting function trying to figure out a way to decrypt the message and anyone can obtain a public key because it is public.
6. A is sure that {M}kb-1 originated with B because it is sending a private key which is only given to the receiver. That key is given to B so A is sure of the authentication.
7. Someone intercepting it can read the message because once they can get into the private key, there is no problem getting the public key.
8. B can ensure authentication as well as confidentiality when sending a message to A by having its private key and also knowing the public key.

Lecture 50

1. A hash function has to be easy to compute for any given data because it should be easy to retrieve the information put in the hash.
2. Strong collision resistance occurs when a function f is hard to find two messages m1 and m2 such that f(m1) = f(m2) while a weak collision resistance occurs when it is hard to find m2 != m3 such that f(m1) = f(m2)
3. Preimage resistance is if given a number, it is hard to find any other number m such that h = f(m) while second preimage resistance is when it is hard to find m2 != m2 such that f(m1) = f(m2)
4. The implications of the birthday attack on a 128 bit hash value is that the attacker needs approximately 2^64 computation to find a collision.
5. The implications of the birthday attack on a 160 bit hash value is that the attacker needs approximately 2^80 computation to find a collision.
6. Cryptographic hash functions are not used for confidentiality due to the transmission of messages in order to confirm that it is actually what was stored is what is being received.
7. Cryptographic hash functions are one-way functions, that's what ensures that message M is bound to H(M) and therefore tamper-resistant
8. B can securely send a message to A and guarantee both confidentiality and integrity will using RSA and cryptographic hash functions by in both, objects can only be contactable at an address that is derived from the secure hash, there is a validity check in using a hash, RSA is a one-way function that makes it impossible to create two objects that could have the same result.

Lecture 51

1. S cannot send the following message because both the sender's key and the receiver's key are both inverses. One needs to be the inverse of the other.

2. S could not have done the encryption in the other order because we are dealing with both authentication and confidentiality. The encryption has to be in the inner bracket because R needs to know it is really S that is sending the messages.
3. Yes, both are the same because the first one is encrypting the message then R is decrypting it and storing it to the sender while the other one is encrypting then decrypting the message but not sending it elsewhere.
4. The requirement of key exchange is that it needs both confidentiality and authentication to be satisfied.

Lecture 52

1. The eavesdropper cannot discover the value (shared secret) even if they know g, p and g^a mod p. They still need b from the receiver to be able to compute it all.
2. The eavesdropper cannot figure out the other numbers if they figured out 'a' the sender's secret number. They still need the prime number, base number and the receiver's secret number.
3. The eavesdropper cannot figure out the other numbers if they figured out 'b' the receiver's secret number. They still need the prime number, base number and the sender's secret number.