Emily Ngo

Emn367

Ngo.emily@utexas.edu

Lecture 34

1. It is impossible to transmit a signal better than C/h because it represents a perfect encoding in a noiseless channel. It is impossible to have a perfect encoding, and also having a rate higher than C/h is over the capacity that a channel can hold.
2. Equivocation is the average uncertainty of what message was actually sent to the recipient due to the noise in the channel. By increasing redundancy the equivocation decreases and also the reliability of the message increases.

Lecture 35

1. Entropy = –(log(1/9))
2. Natural languages are very redundant and also require considering a lot of factors in calculating entropy like when will symbols be independent or dependent of each other. Also, and any estimate of entropy may apply for one text but not others.
3. Zero assumes that all characters all equally likely and independent, first assumes that all characters are independent of one another but each have a probability of occurring; second & third assumes that some characters follow other letter frequently, second order shows 2 letters combos and third order shows 3 letter combos.

Lecture 36

1. Prior probabilities are impossible to compute if the observer does not know the nature of the odds, like the example in lecture how does the observer know beforehand if the nominees are equally likely to win or if the odds aren't even. In order for probabilities to be calculated this must be known.
2. Entropy depends on how much the observers know about the scenario; if the observer knows the outcome then the entropy of the message is 0, if the likelihood of an outcome is equal than it is log(n) where n is the total possibilities; if the odds are uneven then the entropy can't be known until the probabilities are known.
3. Entropy can be used to measure redundancy, if the encoding is closer to its efficient encoding the less redundancy it contains.

Lecture 37

1. The underlying language is probably English if written by Captin Kidd. Also the digits, semicolon, and asterisks are all part of English grammar. The complexity doesn't seem too hard, there is a limited number of symbols and the input text is not too lengthy. The text/content seems kept in its original paragraph structure when looking at the sentence structure. Redundancy is kept in

the encryption. From all of these observations, we are able to infer that the text is most likely English, there are maybe some compression and the nature of the encryption is most likely substitution due to the symbols, structure, and redundancy seen.

2. The encryption already is designed to obscure the meaning of the text. The key is just an extra obstacle you can have to this process. Otherwise the encryption already hides the information content and not the key.
3. Encryption should hide the information content without destroying it, and decryption is retrieving the information content from a noisy channel.
4. Redundancy can reflect between the source text and the encrypted text which a person could use as leverage when trying to decrypt a message. Such as frequencies or regularity of words or characters.

Lecture 38

1. D(E(D(E(P)))) = P
2. D(E(C,KE), KD)
3. Tools like traffic analysis can find clues when you have no idea what the content is but is receiving traffic from a particular entity.
4. Properties of language such as frequencies of vowels or letters can help give away clues, maybe even sentence structure or grammar will show patterns in the encryption.

Lecture 39

1. Although it is breakable, it could take a long time or unreasonable amount of time.
2. An n bit string will produce 2^n possibilities and so when searching for the n bit string you will find it halfway so it will be 2^n-1 operations.
3. Almost all modern commercial symmetric ciphers use some combo of substitution or transposition.
4. Confusion transforms text so you cannot extract original text; diffusion takes the position of the text and moves it around in other positions.
5. A good encryption would utilize both confusion and diffusion, otherwise the encryption strategy may be too naïve to be effective.

Lecture 40

1. Mono means that for every letter ‘a’ it will be replaced by just a ‘b’; poly means for every letter ‘a’ it can be replaced by multiple letters depending on ‘a’s position.
2. However you specify the 1 to 1 mapping for each symbol.
3. Each mapping is 1 to 1 which gives us a k! possible mapping where k is the size of the alphabet.
4. How many positions you shift over from the symbol
5. The size of our alphabet, 26.
6. No, you probably won’t have to try all the possible shifts to decipher a message.
7. You would take a key letter and go to its row and see where the cipher text appears, then take the column letter it corresponds to which will be the plain text.

Lecture 41

1. “xyy” could correspond to any letter, since we do not know if it is a simple substitution, hence 26^3 possibilities.
2. That is because we know that y could only correspond to one letter, so the possibilities are reduced by a factor of 27.
3. Yes, you only need your algorithm to be able to produce probabilities that are equally likely whether or not the attacker knows the cipher text or not.

Lecture 42

1. Even after knowing a cipher text the attacker still have each plaintext equally likely probable, they can’t use their knowledge to reduce search space and has to try all the plaintexts.
2. If the attacker knows the key the search space can be reduced, that is why the key should be random so the attacker can’t use the key for clues.
3. The problem is for this algorithm to work both the sender and receiver need to know the key, however if there was a secure channel such as the key can be passed on then there is no need for a key or an encryption, and if there isn’t a secure channel how does one communicate the key securely? This is the key distribution problem.

Lecture 43

1. Longer text can’t be decrypted unless it has been read entirely which could be a very long time. Character count and frequency is kept in the cipher text, but trigrams and diagrams frequencies at not, so these inferences can be used to indicate that it is a transposition.

Lecture 44

1. Symmetric
2. Distribution management is how to send a key securely, key management is how do we preserve a large number of keys and make them available.
3. Ks is only the public key which is used for encryption, you need the private key in order to decrypt S’s message.
4. Depends, for symmetric encryption you run into key management problems because as the party gets larger the key gets quadratic larger and distribution problem because the key is shared. However, public keys are expensive to generate because of their special structure.

Lecture 45

1. Most modern symmetric encryptions include transposition, so that will make a plaintext required to be read as a block.
2. Malleability for an encryption is bad; it allows the attacker to produce meaningful changes to the plaintext by doing transformations on the cipher text.

3. Homomorphic encrypting allows algebraic computations to a cipher text and generate an encrypted result were it is decrypted will match the operations on the plaintext. This encryption itself is malleable and is used to create secure voting systems.

Lecture 46

1. subBytes uses simple substitution; addroundkey XORs to combine a byte of a state with a byte of the round subkey
2. subRows uses shifts within the rows; mixColumns will mix whole column with matrix multiplication
3. Decryption requires the mixColumn step to be multiplied by the matrix's inverse which can take longer depending on matrix entries.
4. Each block is 128 bits and can profuce 128, 192, or 256 bits depending on the key length. The block is in 4 arrays which will go through 4 steps, subBytes, addroundkey, subRows, or mixColumns depending on the step of the process.
5. Increasing rounds increase with key length so that for large keys every bit affects every ciphertext in a way which disallow measurable differences.

Lecture 47

1. Identical blocks in the plaintext yields identical blocks in the cipher text, and does not hide the content very well.
2. You randomize the blocks first before encrypting it.
3. If the attacker can observe changes they can see the first change on the first block, or content leak where an identical cipher text can be used to derive the plaintext blocks.
4. It will produce random appearing streams of bits. This is used more as a pseudo random number generator.

Lecture 48

1. The decryption key
2. You want the context to be difficult to invert without additional information like not having the decryption key.
3. The public key can be sent freely without worrying out security. Only the receiver can decrypt and not others using the channel.
4. {P}K^-1
5. They are generally much less efficient, public key encryption can take as 10000 as long to prefer as a symmetric encryption because all the operations are complex.

Lecture 49

1. Yes, one factor can be used to find the other.
2. Large primes are used as factors so that one can find the factor easily given the product
3. Yes but it takes a long time

4. Because only A has the decryption key.
5. Anyone could encrypt with the public key.
6. Only B has its decryption key
7. Use B's public key
8. Use a key for authenticity and confidentiality

Lecture 50

1. It has to be done efficiently and quickly for every data type

2. strong is difficult to find 2 messages where f(m1) = f(m2), weak is hard to find m such that h = f(m) or hard to find m2 != m1 such that f(m1) = f(m2)

3. preimage: if given h, hard to find m such that h = f(m); 2nd preimage: hard to find m2 != m1 such that f(m1) = f(m2)

4. 1.25*sqrt(128) bits makes f(m2) = f(m1)

5. 1.25*sqrt(160) bits makes f(m2) = f(m1)

6. Sometimes its not good for integrity

7. Hash function binds bytes of files together

8. Have 2 sets of keys hashed, for authentication and confidentially.

Lecture 51

1. No, S needs to know R's private key

2. Yes, S could have done so vice versa

3. No

4. Key exchange needs confidentiality & authentication

Lecture 52

1. Nothing.

2. The eavesdropper can decode a's messages

3. The eavesdropper can decode b's messages