Name: Neil Jones
EID: nj2977
CSID: nfjones
email: neil.franklin.jones@gmail.com

Week 3 Questions

Lecture 34

1. It would imply that you have beaten the entropy of the language, which isn't possible.

2. You can construct your transmissions such that an incomplete transmission may be reconstructed from the extra information.

Lecture 35

1. h = -(log1/10) = 3.32

2. They contain significant redundancy and require the use of complex models.

3. Zero: ever symbol is assumed to have equal probability.
   First: the probabilities for single symbols are taken into account.
   Second: the probabilities of Diagrams are taken into account.
   Third: the probabilities of trigrams are taken into account.

Lecture 36

1. The number of possibilities may be infinite.

2. The meaning of the information received is based in prior knowledge.

3. The more redundant a language is the lower its entropy will be due to repetition.

Lecture 37

1. Compare character frequencies with known character frequencies in the target language. Are there patterns in the text? This may give insight into the type of encryption used.

2. A key could be optional if the method of encryption is just a substitution cypher. It is extremely easy to break but it doesn't require a key.

3. The information is still all there it just has to be manipulated to be extracted.

4. It can provide insight into the structure of the message.

Lecture 38

1. P

2. $E(P, K_E)$

3. To do traffic analysis. It can represent the urgency of the message.

4. A language with a low entropy may lead to patterns in the encrypted message.

Lecture 39

1. The number of possibilities for the key could be very high. This would make a brute force attack intractable to compute.

2. The probability of each key will be identical. The probability for breaking the cypher will fall in a normal distribution. The expected value will fall in the middle. Since there are 2^n possible keys, the center of the normal distribution will represent 2^{n-1} attempts.

3. It injects confusion into the process. It makes it more difficult to determine the structure of the message.

4. Confusion is transforming information in place while diffusion is moving information around in an orderly way.

5. Both are useful, but diffusion may be more beneficial for eliminating obvious patterns.

Lecture 40

1. Monoalphabetic substitution replaces every symbol with the same corresponding symbol regardless of location while polyalphabetic substitution replaces symbols with multiple symbols depending on the location in the plaintext.

2. The key would be the set of substitution tuples, maybe triples if the substitution is polyalphabetic.

3. Each symbol may be tried once for each corresponding symbol in the true alphabet. So we have n * (n – 1) * (n – 2) * … * 1 = n! Combinatorial possibilities for substitution mapping.

4. the ordinal offset of the mapping (1, 2, .. , n character shift).

5. If k = the size of the alphabet, the keyspace will contain k – 1 possibilities because you can only shift k-1 places without arriving back where you started.

6. No, it would be trivial to break because the keyspace is smaller than the number of symbols in the alphabet.

7. Compute all possible Vigenere Tableeau's and try them.

Lecture 41

1. (26 possible characters)^3

2. If we know that it is a simple substitution cypher then we know that we only need to determine two mappings and that they are independent. So: (26 possibilities) * (25 possibilities).

3. Yes, the key must be as long as the plaintext.

Lecture 42

1. You can't search for patterns if the may is used only once and is as long as the plaintext and the keyspace cannot be cut down.

2. If it isn't random then it leaves it open to prediction.

3. You cannot guarantee that the key isn't being intercepted at some point, ruining the point of encryption in the first place.

Lecture 43

1. The original plaintext is preserved so the letter frequencies are preserved.

Lecture 44

1. The one time pad is symetric because you can get the plaintext by computing XOR with the key and the cyphertext or you can get the cyphertext by computing XOR with the plaintext.

2. Key distribution is getting the key to only those that need it whil management is managing who has access to the key.

3. No, the public key is for encrypting messages sent to S.

4.. Public key systems seem more secure because you don't have to worry as much about key distribution.

Lecture 45

1. It leaves the block size up to chance, making a brute force attack more difficult.

2. You can send secret information to somebody else to perform computations on it.

3. You can compute an operation O(C) and the same operation will be mirrored in the decrypted text D(O(C)) = O(P).

Lecture 46

1. subBytes is a character substitution.

2. mixColumns is a transposition.

3. To decrypt you have to multiply each block by a fixed array, which is a step that is absent from the encryption process.

4. Blocks of bits are sent through rounds of computation which consist of a fixed number of steps.

5. It would increase the deviation from the plaintext and therefore hopefully reduce the likelihood of a reducing the keyspace.

Lecture 47

1. Identical blocks in the plaintext yeild identical blocks in the cypher text.

2. Use each cypher block as the key for the next block.

3. An attacker can analyze the cyphertext for changes in order to determine the first block that changes. The attacker can derive information about plaintext blocks from two identical cyphertext blocks.

4. The cypher is used more as a pseudorandom number generator.

Lecture 48

1. The private key.

2. If the functions were not one-way, the public key could be used to decrypt cyphertext.

3. You can give anybody your public key and they can safely communicate with you without having to know the private key at all.

4. $\{P\}_k^{-1}$

5. Symmetric algorithms are much more efficient because asymmetric encryption algorithms rely on non trivial computations.

Lecture 49

1. Yes, $\{\{P\}_d\}_e = \{\{P\}_e\}_d = P$

2. Using prime numbers makes factoring P^e very difficult.

3. It is not trivially breakable. The keyspace cannot be meaningfully reduced.

4. They don't have the private key.

5. Anybody can have the public key.

6. Only B can have the private key.

7. Use the public key to decrypt it.

8. You could use digital signatures.

Lecture 50

1. It has to be computed many times.

2. m_1 and m_2 may be equal in a string collision resistant function.

3. In preimage resistance we are only concerned with the hash value of one message, while in second preimage resistance we are concerned with multiple messages.

4. The an equal hash will be found after about 14.14 arguments.

5. “ 15.81 “

6. They are easy to break.

7. The function f is invariant on specific input. f(M) will always produce the same hash value.

8. B sends the message to A. A hashes the message. B sends the message again and A checks the hash values. Digital signatures must be used.

Lecture 51

1. Yes, only R can decrypt it and only S could have encrypted it.

2. Yes, both parties stilll have to use the same keys to encrypt/decrypt.

3. No, it is equivalent to $\{K\}_R$

4. They require both confidentiality and authentication. You have to know that the person you are sending the key to is the right one and you have to know that it can only be read by them.

Lecture 52

1. The eavesdropper wouldn't be able to decrypt the message in a reasonable amount of time.

2. It would make it easier to discover the message by reducing the key space.

3. Same as 2.