Name:Vincent Nguy

EID:vn2863

CS Login:vn2863

Email:nguyvincent@yahoo.com

# CS361 Questions: Week 3

The questions marked with a dagger (†) require external research and may be more extensive and time consuming. You don’t have to do them for the assignment but, but do them to increase your competency in the class.

# Lecture 34

1. Why is it impossible to transmit a signal over a channel at an average rate greater than C/h?

C is the max bits a channel can transmit, and h is the entropy of a language so then C/h would be the greatest rate possible.

1. How can increasing the redundancy of the coding scheme increase the reliability of transmitting a message over a noisy channel?

# Lecture 35

1. If we want to transmit a sequence of the digits 0-9. According to the zero order model, what is the entropy of the language?

h = -(log(1/10))

1. What are reasons why computing the entropy of a natural language is difficult?

It is difficult in finding the exact probability of the possible n cominations at the nth level order.

1. Explain the difference between zero, first, second and third-order models.

Zero order – assume all characters are equally likely when you compute the entropy

First order-assume some symbols occur more frequently than others, but all symbols are still independent.

2nd order- you can computed a table of likelihoods of diagrams(two-letter combinations)

3rd order – same as 2nd order but adding trigrams (three letter combinations).

# Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

You don’t

1. Why is the information content of a message relative to the state of knowledge of an observer?

If the observer already knows the information in the message the entropy would be 0 since they have no uncertainty.

1. Explain the relationship between entropy and redundancy.

Note that entropy can be used to measure the amount of “redundancy” in the encoding. If the information content of a message is equal to the length of the encoded message, there is no redundancy.

# Lecture 37

1. List your observations along with their relevance to cryptography about Captain Kidd’s encrypted message.

It’s encoded in symbols and numbers, and there are a lot of 8’s

1. Explain why a key may be optional for the processes of encryption or decryption.

You can do it without.

1. What effect does encrypting a file have on its information content?

It protects it from unwanted viewers and should be able to be recreated.

1. How can redundancy in the source give clues to the decoding process?

You can use patterns. To spot the possible language the plaintext is in.

# Lecture 38

1. Rewrite the following in its simplest form: *D*(*E*(*D*(*E*(*P*)))).

{{{{P}}}}

1. Rewrite the following in its simplest form: *D*(*E*(*E*(*P,KE*)*,KE*)*,KD*).

{{P}Ke}Ke}Kd

1. Why might a cryptanalyst want to recognize patterns in encrypted messages?

Patterns can give us clues in what language the message is in.

1. How might properties of language be of use to a cryptanalyst?

You can spot traits of languages that may have not been removed after being encoded.

# Lecture 39

1. Explain why an encryption algorithm, while breakable, may not be feasible to break?

You can always brute force all possible keys to break the encryption but it may take too long for it to be feasible.

1. Why, given a small number of plaintext/ciphertext pairs encrypted underkey K, can K be recovered by exhausteive search in an expected time on the order of 2*n*−1 operations? Because there are 2^n possibilities and if you do a linear search the average search space would be half of that leading to 2^(n-1) operations.
2. Explain why substitution and transposition are both important in ciphers.

Substitution will provide Confusion to encryption, and transposition will provide Diffusion.

1. Explain the difference between confusion and diffusion.

Confusion – transforming information in plaintext so that an interceptor cannot readily extract it.

Diffusion – spreading the information from a region of plaintext widely over the ciphertext.

1. Is confusion or diffusion better for encryption?

Both are good for encryption and would be best to employ both.

# Lecture 40

1. What is the difference between monoalphabetic and polyalphabetic substitution?

Monoalphabetic – a uniformly 1-1 mapping.

Polyalphabetic-

1. What is the key in a simple substitution cipher?

A 1-1 mapping from a plaintext to ciphertext.

1. Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?

It is a permutation without repetition which would mean for k letters would lead to a k! mappings.

1. What is the key in the Caesar Cipher example?

A = C, B = D, C = E,….. , Y = A, Z = B.

1. What is the size of the keyspace in the Caesar Cipher example?

26

1. Is the Caesar Cipher algorithm strong?

No this algorithm is pretty easy to break.

1. What is the corresponding decryption algorithm to the Vigenere ciphertext example?

Using the Vigenère Tableau means that you are using one of twenty-six different Caesar Ciphers at each position, depending upon the corresponding letter in the key.

# Lecture 41

1. Why are there 17576 possible decryptions for the “xyy” encoding on slide3?

We only know it’s a substitution so there are 26\*26\*26 possibilities.

1. Why is the search space for question 2 on slide 3 reduced by a factor of 27?

Because it was a simple substitution cipher so it’s 1-1 mapping ending with 26\*25 possibilities

1. Do you think a perfect cipher is possible? Why or why not?

Yes, but you would have to have a fully random generated key.

# Lecture 42

1. Explain why the one-time pad offers perfect encryption.

With a random key and plaintext is XOR creating a cipher text therefore you can’t remove any of the possible plaintext cause they could be a possible pre image of the cipher text.

1. Why is it important that the key in a one-time pad be random?

If not you could take the cipher text + the key and decode it yourself.

1. Explain the key distribution problem.

How do the sender and reciver agree on a secret(key) that they could use.

**Lecture 43**

1. What is a downside to using encryption by transposition?

Unlike simple substitution, it has greater space complexity since the message can’t be decrypted until it has been read in its entirety. This may be an issue for very long messages, and causes a delay in the decryption.

# Lecture 44

1. Is a one-time pad a symmetric or asymmetric algorithm?

It’s symmetric

1. Describe the difference between key distribution and key management.

Key distribution: how do we convey keys to those who need them to establish secure communication.

Key management: given a large number of keys, how do we preserve their safety and make them available as needed

1. If someone gets a hold of Ks, can he or she decrypt S’s encrypted messages? Why or why not?

No for an asymmetric encryption the encrypt key and decrypt key is different.

1. Are symmetric encryption systems or public key systems better?

Public key systems.

# Lecture 45

1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?

Block ciphers are has a better immunity to tampering. It’s difficult to insert symbols without detection.

1. What is the significance of malleability?

It’s bad for encryption. If an encryption algorithm has malleability a person can decode your plaintext without detection

1. What is the significance of homomorphic encryption?

Homomorphic encryption is a form of encryption where a specific algebraic operation performed on the plaintext is equivalent to another (possibly different) algebraic operation performed on the ciphertext. Homomorphic encryption schemes are malleable by design.

# Lecture 46

1. Which of the 4 steps in AES uses confusion and how is it done?

subBytes - or each byte in the array, use its value as an index into a 256-element lookup table, and replace its value in the state by the byte value stored at that location in the table.

1. Which of the 4 steps in AES uses diffusion and how is it done?

shiftRows –Let *Ri* denote the *ith* row in state. Shift *R*0 in the state left 0 bytes (i.e., no change); shift *R*1 left 1 byte; shift *R*2 left 2 bytes; shift *R*3 left 3 bytes. This does not affect the individual byte values themselves.

1. Why does decryption in AES take longer than encryption?

The inverse array in Inverse Mix Columns step in decryption has numbers that isn’t easily optimized making decryption take longer.

1. Describe the use of blocks and rounds in AES.

A implementation of a round is called a iterated block cipher, where a block is used to store data where then steps of encryption are iterated to for a certain number of rounds.

1. Why would one want to increase the total number of Rounds in AES?

It could lead to a harder to crack encryption.

# Lecture 47

1. What is a disadvantage in using ECB mode?

If you have Identical blocks in the plaintext it would generated identical blocks in the ciphertext.

1. How can this flaw be fixed?

By using a randomize plaintext block before encrypting

1. What are potential weaknesses of CBC?

A person can observed changes to ciphertext overtime, content leak, if an attacker can find two identical ciphertext block.

1. How is key stream generation different from standard block encryption modes?

In block encryption modes (like ECB and CBC), the point is to generate ciphertext that stores the message in encrypted but recoverable form. In key stream generation modes the cipher is used more as a pseudorandom number generator. The result is a key stream that can be used for encryption by XORing with a message stream. Decryption uses the same key stream.

# Lecture 48

1. For public key systems, what must be kept secret in order to ensure secrecy?

A Secret key to decrypt.

1. Why are one-way functions critical to public key systems?

It makes decrypting a message hard without knowing the secret key.

1. How do public key systems largely solve the key distribution problem?

It is ok to for your public key to be leaked even though you can encrypted with it no one but the person with the corresponding secret key can decrypt it.

1. Simplify the following according to RSA rules: {{{*P*}*K*−1}*K*}*K*−1.
2. Compare the efficiency of asymmetric algorithms and symmetric algorithms.

Asymmetric algorithms are generally less efficient than symmetric algorithms.

# Lecture 49

1. If one generated new RSA keys and switched the public and private keys, would the algorithm still work? Why or why not?

Yes. A plaintext block *P* is encrypted as (*Pe* mod *n*). The decrypting key is chosen so that: (*Pe*)*d* mod *n*=*P*. Because the encrypting exponentiation is performed modulo *n*, an interceptor would have to factor *Pe* to recover the plaintext. This is difficult. However, the legitimate receiver knows *d* and merely computes (*Pe*)*d* mod *n*=*P*. This is much easier.

1. Explain the role of prime numbers in RSA.

It w

1. Is RSA breakable?

The algorithm is theoretically secure, but has practical weaknesses so possibly.

1. Why can no one intercepting {*M*}*Ka* read the message?

Only A has the key to allow decryption

1. Why can’t A be sure {*M*}*Ka* came from B?

Anyone could have A’s public key

1. Why is A sure {*M*}*K*−1 originated with B?

*B*

*Because this is encrypted with b’s private key and only B has that*

1. How can someone intercepting {*M*}*K*−1 read the message?

*B*

*Anybody can have B’s public key and can capture the message .*

1. How can B ensure authentication as well as confidentiality when sending a message to A?

By having two pairs of keys, one for privacy and one for signing.

# Lecture 50

1. Why is it necessary for a hash function to be easy to compute for any given data?
2. What is the key difference between strong and weak collision resistance of a hash function.

Strong its hard to find two messages m1 and m2 such that f(m1) = f(m2),

Weak its hard to find a m2 != m1 such that f(m1) = f(m2).

1. What is the difference between preimage resistance and second preimage resistance?

For pre-image given a hash value its hard to find a message that hashes to that value. For 2nd pre-image if we already have a message and its hash value and its difficult to find another message that hashes to the same value.

1. What are the implications of the birthday attack on a 128 bit hash value?

1.25sqrt(2^128) = 1.25(2^64)

1. What are the implications of the birthday attack on a 160 bit hash value?

1.25sqrt(2^160) = 1.25(2^80)

1. Why aren’t cryptographic hash functions used for confidentiality?

It’s usually used for integrity.

1. What attribute of cryptographic hash functions ensures that message M isbound to *H*(*M*), and therefore tamper-resistant?

Each time the file is access we compare the has function value from last time vs this access.

1. Using RSA and a cryptographic hash function, how can B securely send a message to A and guarantee both confidentiality and integrity?

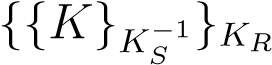
# Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following message: {{*K*}*KS*−1}*K*−1? Why or why not?

Yes since all you need is S’s public key.

1. In the third attempt at key exchange on slide 5, could S have done the encryptions in the other order? Why or why not?

No if it was done the other way people could get S’s private key and his encryption is protected.

1. Is {{{*K*}*KS*−1}*KR*}*KS* equivalent to?

Yes.

1. What are the requirements of key exchange and why?

A RSA key pair.

# Lecture 52

1. What would happen if g, p and *ga*mod*p* were known by an eavesdropper listening in on a Diffie-Hellman exchange?

They would be able to break your encryption.

1. What would happen if a were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?

They could listen to messages being sent to B

1. What would happen if b were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?

They could listen to messages being sent to A