Adan Cortez

AC42886

Lecture 34

1. Why is it impossible to transmit a signal over a channel at an average rate

greater than C/h?

C/h is considered the upper limit as well as the perfect encoding for a given language. It is not possible to obtain a perfect encoding but it is possible to get arbitrarily close to it. To exceed this limit means that you have found a way to send information in less bits than told by entropy or the channel is now sending more than its capacity.

2. How can increasing the redundancy of the coding scheme increase the reliability

of transmitting a message over a noisy channel?

The increased redundancy can make it easier for the receiver to decode regardless of the noise introduced into the message. If there's any bandwidth, then increased repetition and redundancy can help get a message across the channel eventually.

Lecture 35

1. If we want to transmit the numbers 0-9, using a zero-order model, what is

the entropy of the language?

h = -(log(1/10)) = 3.321928

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

Computing the entropy of a natural language involves many complex models and involves experimenting with arbitrarily high order models only to compute an estimate.

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

Zero order models assume equal likelyhood for all input symbols. First order models assume that all symbols are independent of each but has some probability involved. Second order models takes into account the likelyhood that a letter will follow a given letter. Third order models takes into account the likelyhood that a letter will follow 2 given letters. And so on and so forth for higher order models.

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

It's hard to know about prior probabilities since it requires complex modeling that takes information known beforehand about the context at hand.

2. Why is the information content of a message relative to the state of knowledge

of an observer?

The information content is only there to help the receiver obtain information without any uncertainty. If the observer knows the probabilities of something occuring, then he can narrow the choices or if he already knows what will happen, then he doesn't need any information content to resolve uncertainty.

3. Explain the relationship between entropy and redundancy.

Entropy and redundancy are inversely related. That is the closer the information content is to the entropy, the less redundancy there is in the encoding and vice-versa.

Lecture 37

1. List your observations along with their relevance to cryptography about

Captain Kidd’s encrypted message.

What's the underlying language of the encrypted message so we know what kind of information content it was originally supposed to have? What context is the encrypted message referring to? Can we assuming directional text or something else? How common are particular sequences in the encrypted message? Can we assume these correlate to some decrypted text? How complex is the encryption? What kind of complexity is the person capable of? Have any compressions been made to the message that would alter the encrypted message?

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

An encryption and decryption doesn't necessarily need a key but without the key able to randomize the process, any attacker that can recognize the function used can easily decrypt it as well making it very unpractical and unsafe.

3. What effect does encrypting a message have on the information content of a file?

The encryption should render the message less useful to any eavesdroppers but should preserve the information content of the file. Otherwise, it is not possible to extract the information content from the file.

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

If the encrypted text has redundancies that are reflected in the source, then the attacker can use that to leverage for decrypting the message. Like in the pirate example, the letter e is the most common and one can use that knowledge to see how redundant a sequence is and substitute that sequence accordingly.

Lecture 38

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

D(E(D(E(P)))) = D(E(P)) = P

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

D(E(E(P,KE),KE),KD) = D(E(E(P,KE),KE),KD) = E(P,KE)

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

Patterns in encrypted messages tend to give clues about a given scenario.

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

Some languages always have a higher frequency of a given symbol. It is possible to decrypt a message based on that known frequency.

Lecture 39

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

to break?

Some modern standard algorithms have up to 256bits strings as a key. That gives us impossibly many choices to have to brute force through to find a correct key. Given enough time it is possible but it may take several years or decades before an answer is returned.

2. Why, given a small number of plaintext/ciphertext pairs encrypted under

key K, can K be recovered by exhaustive search in an expected time on the

order of 2^(n−1) operations?

A person could brute force through all possible keys of length n given that a person can recognize a success. The small number of plaintext and ciphertext gives the attacker a input and output to go by so he could encrypt the plaintext using a random key to test and see if it matches with the ciphertext. In order to try all possiblities, the attacker must try 2^(n-1) keys.

3. Explain why substitution and transposition are both important in ciphers.

Substitution exchanges one symbol for another while transposition rearranges the order of symbols. Most modern commercial ciphers use a complicated combination of these two building blocks. Substitution tends to confuse any potential attackers and transposition tends tospread the information over the ciphertext.

4. Explain the difference between confusion and diffusion.

Confusion transforms the infromation in a way that it is not readily extractable. Diffusion spreads the information from a region of plaintext widely over the ciphertext.

5. Is confusion or diffusion better for encryption?

It depends on the context. Both are important to encryption as both are essential to ensuring that there is as few leverages as possible for an attacker to notice. If only one was allowed, then confusion would be best to attempt to make thet information as hard as possible to readily extract.

Lecture 40

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

Monoalphabetic substitution is done uniformly throughout all symbols in the plaintext. Polyalphabetic substitution is done depending on where in the plaintext that the symbol occurs.

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

The key in a simple substitution cipher is a one to one mapping of symbols.

3. Why are there k! mappings from plaintext to ciphertext alphabets in simple

substitution?

Since there are k choices for mapping in substitution, we have k choices for the first mapping. Followed by k-1 for the second mapping, k-2 for the third mapping and so on. The total number of possible keys therefore is k\*(k-1)\*(k-2)..... which is k!.

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

The key is a one to one mapping where the symbol in the plaintext is replaced in the encryption by another letter a fixed distance away in the alphabet.

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

The size of the key space is k or k-1 symbols where k is the size of the alphabet.

6. Is the Caesar Cipher algorithm strong?

No. It probably isn't necessary to try all k combinations to figure it out.

7. What is the corresponding decryption algorithm to the Vigenere ciphertext

example?

If the key is known, then it is possible to decrypt by looking for the row or column containing the key symbol and find the ciphertext symbol and the intersecting row or column.

Lecture 41

1. Why are there 17576 possible decryptions for the “xyy” encoding on slide 3?

Since it is not stated that it is a simple substitution cipher, it could have 26 choices for each of the 3 symbols which is 26^3 or 17576 possibilities.

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

If it is a simple substitution cipher, then you know that "xyy" only has 2 distinct symbols and the same symbol substitution cannot be reused. So there are 26 choices for "x" and 25 choices for "y". Therefore there are a total of 26\*25 = 650 possibilities.

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

If there is a "perfect" cipher, it would have to be polyalphabetic in its substitution to prevent any facts about the language such as the frequency of more common letters like "e" to be known and provide leverage to the attacker. The key would also have to be randomly generated, as any keys, which have a higher frequency in some parts, would also provide leverage.

Lecture 42

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

It is not possible to reduce the search space for the message or the key since the key is one time use and random. Therefore the only way to break one-time padding is to brute force all possibilities.

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

If any facts are known about the key, then the attacker can use that information to leverage against the ciphertext and decrease the search space.

3. Explain the key distribution problem.

The sender and receiver must share the key in order to be able to encrypt and decrypt the message. In order to send the key, there must be a secret or secure way to do it. If there is, then why not use the secure channel. If there isn't, then how can you share the key securely.

Lecture 43

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

Transposition only reorders characters but doesn't replace them. Therefore, the original characters still occur in the result.

2. How could a combination of ciphers be weaker than the individual ciphers

alone?

For example, encrypting paintext using a caesar cipher and then encrypting that ciphertext with another caesar cipher may return the plaintext if the sum of shifts is equivalent to the size of the lphabet.

Lecture 44

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

One-time pad is a symmetric algorithm.

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

In key distrobution, we deal with the problem of how to convey keys to those who need them to establish secure connection. In key management, we deal with the problem of how to preserve and assure aavailability of a large number of keys.

3. If someone gets a hold of Ks, can he or she decrypt S’s encrypted messages?

Why or why not?

In asymmetric encryption, having Ks does not allow anyone to decrypt the message. Only the receiver holds the private key which can decrypt the message.

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

Symmetric encryption systems are more secure and easier and cheaper to generate keys than asymmetric encryption systems. Asymmetric systems have significantly less key management to worry about. For performance, asymmetric systems would be better. For security, symmetric systems would be better.

Lecture 45

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

block ciphers?

Block ciphers add on immunity to tampering which is fundamental to ensuring the integrity of information. It also adds high diffusion to prevent any "weak" spots to leverage from in the ciphertext. In a sense, stream encryption is easier to calculate while blocciphers tend to be more secure.

2. What is the significance of malleability? What is the significance of

homomorphic encryption?

If an encryption system is malleable, then changes in the ciphertext result in meaningful changes to the plaintext. For the sake of integrity, having a malleable system is not desired. Homomorphic encryption allows for third parties to manipulate encrypted data and perform calculations on it and the owner is then able to decrypt that manipulated data and give the answer to the necessary parties. This is useful to allow third parties to work with the encrypted information without ever releasing the information.

Lecture 46

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

The step for confusion is subBytes. For every byte in the array, it uses its value as an index into a 256-element lookup table and replaces the byte by the value stored at the table location. MixColumns adds confusion as well by multiplying each column within the matrix by a fixed matrix of integers.

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

The step for diffusion is shiftRows. Like the name says, it shifts the rows within the matrix by a different amount for each row.

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

In the mixColumn step, you have to multiple by the inverse of the matrix which has more complicated numbers to multiply by.

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

The blocks designate a size of data to be encrypted where it can be arranged and handled by the encryption method. The rounds tell the method how many passes it must make.

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

The higher the number of rounds, the more mangled the data becomes. The more mangled data becomes, the less likely the attacker can leverage any information from it.

Lecture 47

1. What is a disadvantage in using ECB mode?

ECB result in identical blocks in the ciphertext if the same plaintext is used constantly since the keys are reused for every block.

2. How can this flaw be fixed?

By using Cipher Block Chaining to XOR each sucessive plaintext block with the previous ciphertext block.

3. What are potential weaknesses of CBC?

An attacker is able to observer changes to the ciphertext over time and is able to spot the first block that changed. If an attacker can find two identical ciphertext blocks, he can derive the XOR of the plaintext by XORing the 2 ciphertexts and derive info about the two-plaintext blocks.

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

The key stream generation uses encryption algorithms to generate random appearing streams of bits to use as a one-time pad.

Lecture 48

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

The private key used for decrypting messages.

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

The messages sent must be easy to encrypt for any user but hard to decrypt for anyone who does not possess the secret key.

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

The public key allows the person wanting to receive messages to send the key in the open without caring for any eavesdroppers. In that case, only the person who has the secret key can decrypt any messages that come to him.

4. Simplify the following according to RSA rules: {{{P}−1 K }K}K−1.

{{P}−1 K }

5. Compare the efficiency of asymmetric algorithms and symmetric algorithms.

An asymmetric algorithm such as the public key encryption may take up to 10,000 times longer to perform than symmeetric encryption since asymmetric algorithms don't use bitwise operations and rely on factoring and modular exponentiation.

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. The key are used in a symmetric fashion where either encrypting a decryption or decrypting an encryption yields the same message.

2. Explain the role of prime numbers in RSA.

RSA relies on large primes for their diffculty in being to factor their product easily and quickly.

3. Is RSA breakable?

RSA is still breakable through a brute force method.

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

Only A has the key that can decrypt the message.

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

Since the key used to encrypt it is public, there's no way to verify that the encrypted message came from B.

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

Only B has the secret key able to encrypt the message sent to A where A is able to decrypt it using the public key

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

Any one intercepting the message can just use B's public key to decrypt the message sent to A.

8. How can B ensure authentication as well as confidentiality when sending a

message to A?

If B is using RSA, he can encrypt something with the private key to send to A and then consequently encrypt it again using A's public key. That way only A can decrypt the top layer and then authenticate the second layer.

Lecture 50

1. Why is it necessary for a hash function to be easy to compute for any given

data?

A hash must be able to easily produce a fixed size integer given any size of text in order to be useful in quick integrity checks.

2. What is the key difference between strong and weak collision resistance of

a hash function.

Weak collision deals with collisions given a particular input. Strong collision deals with collisions given any input.

3. What is the difference between preimage resistance and second preimage

resistance?

Preimage resistance says given any hash, it is hard to find a message that hashes to that hash value. Second preimage resistance states that given any input, it is hard to find another input to where they share the same hash.

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

You have to look at 1.25\*2^64 values before finding a collision.

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

You have to look at 1.25\*2^80 values before finding a collision.

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

Cryptographic hash functions are unreversible so you cannot hide any information in a hash without destroying it.

7. What attribute of cryptographic hash functions ensures that message M is

bound to H(M), and therefore tamper-resistant?

Collision resistance is what allows messages to be bound to their respective hashes.

8. Using RSA and a cryptographic hash function, how can B securely send a

message to A and guarantee both confidentiality and integrity?

B can use A's public key to send a message with confidentiality and then send a hash of that message for A to be able to perform his own hash and compare with.

Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following

message: {{K}KS−1}KR−1? Why or why not?

No, both layers are encrypted using private keys meaning any eavesdropper can easily decrypt both layers using public keys from both R and S.

2. 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, in the other order, the top layer could easily be stripped off by an eavesdropper which nullifies any authentication.

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

No, it is lacking one layer of encryption without any private key to warrant negating that layer.

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

Key exchange requires both confidentiality and authentication. In order to use the key, you must ensure that no one has seen the key other than the receiver and you must ensure that the key comes from a valid source and not a malicious source.

Lecture 52

1. What would happen if g, p and g^a mod p were known by an eavesdropper

listening in on a Diffie-Hellman exchange?

Nothing. Brute forcing it for the shared key would take infinity time.

2. What would happen if a were discovered by an eavesdropper listening in on

a Diffie-Hellman exchange?

If a was discovered, then the eavesdropper can essentially take the place of Alice and calculate everything in her place.

3. What would happen if b were discovered by an eavesdropper listening in on

a Diffie-Hellman exchange?

If b was discovered, then the eavesdropper can essentially take the place of Bob and calculate everything in his place.