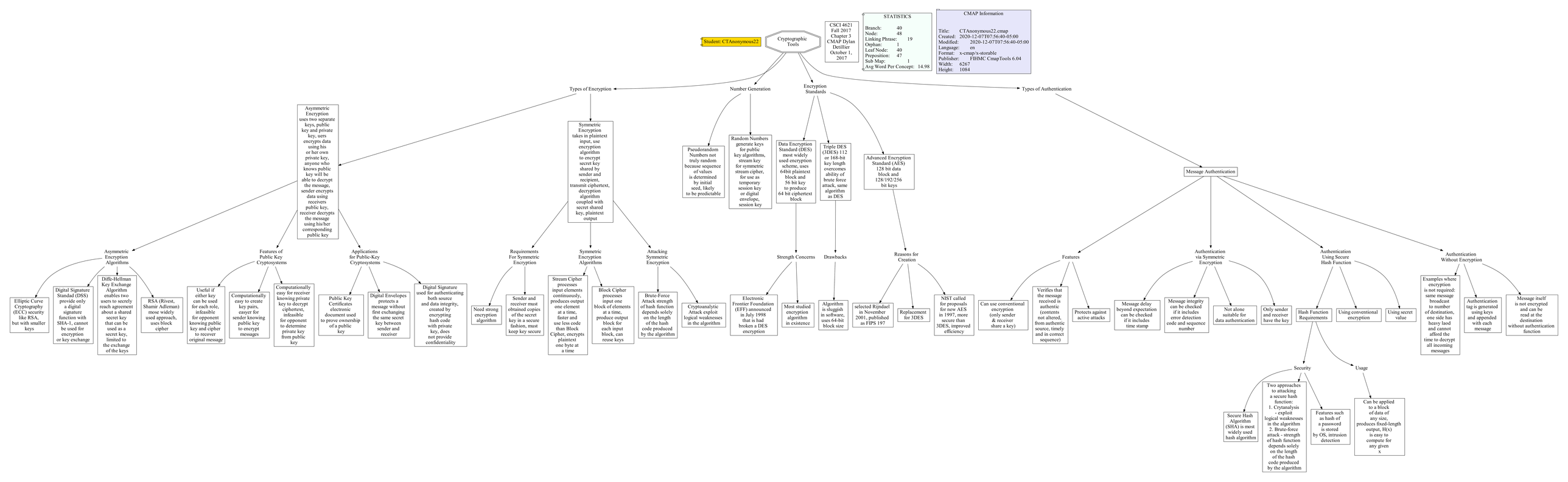
Student: CTAnonymous22
Cryptographic Tools
CSCI 4621
Fall 2017
Chapter 3
CMAP Dylan Deitllier
October 1, 2017
STATISTICS
Branch: 40
Node: 48
Linking Phrase: 19
Orphan: 1
Leaf Node: 40
Preposition: 47
Sub Map: 1
Avg Word Per Concept: 14.98
CMAP Information
Title: CTAnonymous22.cmap
Created: 2020-12-07T07:56:40-05:00
Modified: 2020-12-07T07:56:40-05:00
Language: en
Format: x-cmap/x-storable
Publisher: FIHMC CmapTools 6.04
Width: 6267
Height: 1084
Types of Encryption
Number Generation
Encryption Standards
Types of Authentication
Asymmetric Encryption uses two separate keys, public key and private key, uers encrypts data using his or her own private key, anyone who knows public key will be able to decrypt the message, sender encrypts data using receivers public key, receiver decrypts the message using his/her corresponding public key
Symmetric Encryption takes in plaintext input, use encryption algorithm to encrypt secret key shared by sender and recipient, transmit ciphertext, decryption algorithm coupled with secret shared key, plaintext output
Pseudorandom Numbers not truly random because sequence of values is determined by initial seed, likely to be predictable
Random Numbers generate keys for public key algorithms, stream key for symmetric stream cipher, for use as temporary session key or digital envelope, session key
Data Encryption Standard (DES) most widely used encryption scheme, uses 64bit plaintext block and 56 bit key to produce 64 bit ciphertext block
Triple DES (3DES) 112 or 168-bit key length overcomes ability of brute force attack, same algorithm as DES
Advanced Encryption Standard (AES) 128 bit data block and 128/192/256 bit keys
Message Authentication
Asymmetric Encryption Algorithms
Features of Public Key Cryptosystems
Applications for Public-Key Cryptosystems
Requirements For Symmetric Encryption
Symmetric Encryption Algorithms
Attacking Symmetric Encryption
Strength Concerns
Drawbacks
Reasons for Creation
Features
Authentication via Symmetric Encryption
Authentication Using Secure Hash Function
Authentication Without Encryption
Elliptic Curve Cryptography (ECC) security like RSA, but with smaller keys
Digital Signature Standad (DSS) provide only a digital signature function with SHA-1, cannot be used for encryption or key exchange
Diffe-Hellman Key Exchange Algorithm enables two users to secrely reach agreement about a shared secret key that can be used as a secret key, limited to the exchange of the keys
RSA (Rivest, Shamir Adleman) mose widely used approach, uses block cipher
Useful if either key can be used for each role, infeasible for opponent knowing public key and cipher to recover original message
Computationally easy to create key pairs, easyer for sender knowing public key to encrypt messages
Computationally easy for receiver knowing private key to decrypt ciphertext, infeasible for opponent to determine private key from public key
Public Key Certificates electronic document used to prove ownership of a public key
Digital Envelopes protects a message without first exchanging the same secret key between sender and receiver
Digital Signature used for authenticating both source and data integrity, created by encrypting hash code with private key, does not provide confidentiality
Need strong encryption algorithm
Sender and receiver must obtained copies of the secret key in a secure fashion, must keep key secure
Stream Cipher processes input elements continuously, produces output one element at a time, faster and use less code than Block Cipher, encrypts plaintext one byte at a time
Block Cipher processes input one block of elements at a time, produce output block for each input block, can reuse keys
Brute-Force Attack strength of hash function depends solely on the length of the hash code produced by the algorithm
Cryptoanalytic Attack exploit logical weaknesses in the algorithm
Electronic Frontier Foundation (EFF) announced in July 1998 that is had broken a DES encryption
Most studied encryption algorithm in existence
Algorithm is sluggish in software, uses 64-bit block size
selected Rijndael in November 2001, published as FIPS 197
Replacement for 3DES
NIST called for proposals for new AES in 1997, more secure than 3DES, improved efficiency
Can use conventional encryption (only sender & receiver share a key)
Verifies that the message received is authentic (contents not altered, from authentic source, timely and in correct sequence)
Protects against active attacks
Message delay beyond expectation can be checked if it includes time stamp
Message integrity can be checked if it includes error detection code and sequence number
Not alone suitable for data authentication
Only sender and receiver have the key
Hash Function Requirements
Using conventional encryption
Using secret value
Security
Usage
Secure Hash Algorithm (SHA) is most widely used hash algorithm
Two approaches to attacking a secure hash function: 1. Crytanalysis - exploit logical weaknesses in the algorithm 2. Brute-force attack - strength of hash function depends solely on the length of the hash code produced by the algorithm
Features such as hash of a password is stored by OS, intrusion detection
Can be applied to a block of data of any size, produces fixed-length output, H(x) is easy to compute for any given x
Examples where encryption is not required: same message broadcast to number of destination, one side has heavy load and cannot afford the time to decrypt all incoming messages
Authentication tag is generated using keys and appended with each message
Message itself is not encrypted and can be read at the destination without authentication function