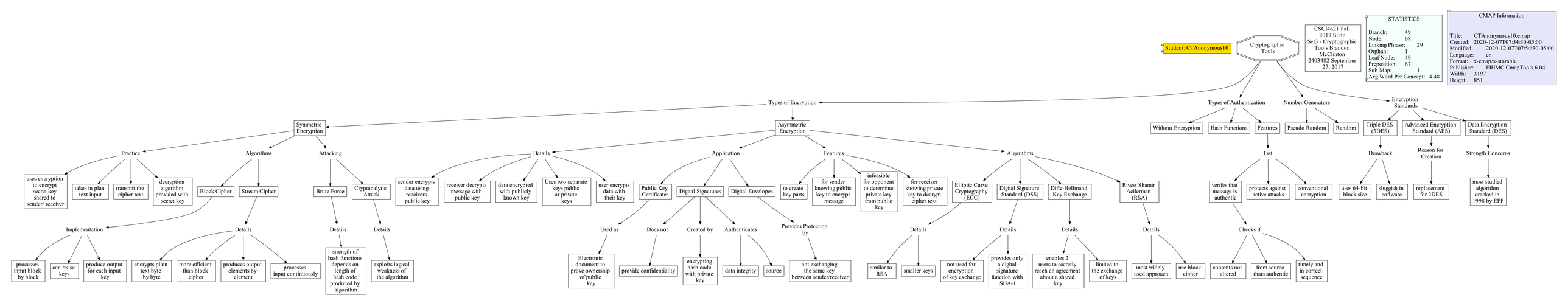
Student: CTAnonymous10
Cryptographic Tools
CSCI4621 Fall 2017 Slide Set3 - Cryptographic Tools Brandon McClinton 2403482 September 27, 2017
STATISTICS
Branch: 49
Node: 68
Linking Phrase: 29
Orphan: 1
Leaf Node: 49
Preposition: 67
Sub Map: 1
Avg Word Per Concept: 4.48
CMAP Information
Title: CTAnonymous10.cmap
Created: 2020-12-07T07:54:30-05:00
Modified: 2020-12-07T07:54:30-05:00
Language: en
Format: x-cmap/x-storable
Publisher: FIHMC CmapTools 6.04
Width: 3197
Height: 851
Types of Encryption
Symmetric Encryption
Practice
uses encryption to encrypt secret key shared to sender/ receiver
takes in plan text input
transmit the cipher text
decryption algorithm provided with secret key
Algorithms
Block Cipher
Stream Cipher
Implementation
processes input block by block
can reuse keys
produce output for each input key
Details
encrypts plain text byte by byte
more efficient than block cipher
produces output elements by element
processes input continuously
Attacking
Brute Force
Cryptanalytic Attack
Details
strength of hash functions depends on length of hash code produced by algorithm
Details
exploits logical weakness of the algorithm
Asymmetric Encryption
Details
sender encrypts data using receivers public key
receiver decrypts message with public key
data encrypted with publicly known key
Uses two separate keys public or private keys
user encrypts data with their key
Application
Public Key Certificates
Digital Signatures
Digital Envelopes
Used as
Electronic document to prove ownership of public key
Does not
provide confidentiality
Created by
encrypting hash code with private key
Authenticates
data integrity
source
Provides Protection by
not exchanging the same key between sender/receiver
Features
to create key parts
for sender knowing public key to encrypt message
infeasible for opponent to determine private key from public key
for receiver knowing private key to decrypt cipher text
Algorithms
Elliptic Curve Cryptography (ECC)
Digital Signature Standard (DSS)
Diffe-Hellmand Key Exchange
Rivest Shamir Acilerman (RSA)
Details
similar to RSA
smaller keys
Details
not used for encryption of key exchange
provides only a digital signature function with SHA-1
Details
enables 2 users to secretly reach an agreement about a shared key
limited to the exchange of keys
Details
most widely used approach
use block cipher
Types of Authentication
Without Encryption
Hash Functions
Features
List
verifies that message is authentic
Checks if
contents not altered
from source thats authentic
timely and in correct sequence
protects against active attacks
conventional encryption
Number Generators
Pseudo Random
Random
Encryption Standards
Triple DES (3DES)
Drawback
uses 64-bit block size
sluggish in software
Advanced Encryption Standard (AES)
Reason for Creation
replacement for 2DES
Data Encryption Standard (DES)
Strength Concerns
most studied algorithm cracked in 1998 by EFF