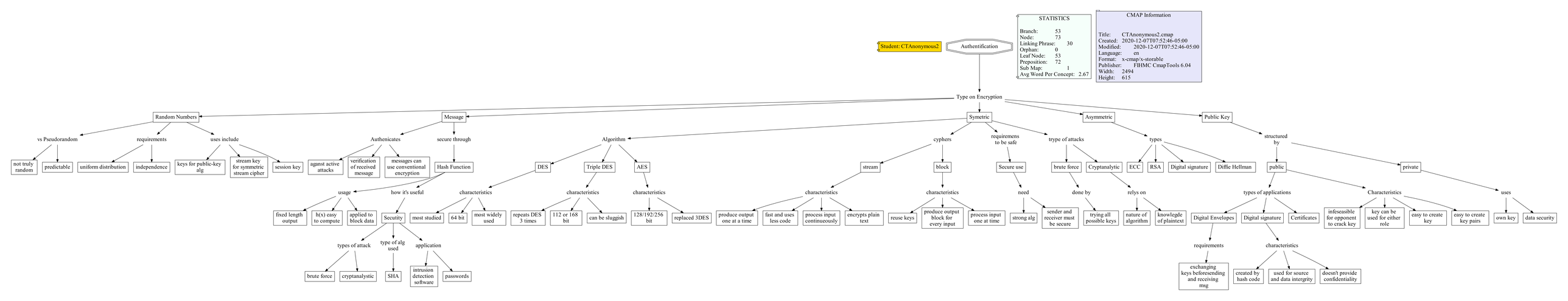
Student: CTAnonymous2
Authentification
STATISTICS
Branch: 53
Node: 73
Linking Phrase: 30
Orphan: 0
Leaf Node: 53
Preposition: 72
Sub Map: 1
Avg Word Per Concept: 2.67
CMAP Information
Title: CTAnonymous2.cmap
Created: 2020-12-07T07:52:46-05:00
Modified: 2020-12-07T07:52:46-05:00
Language: en
Format: x-cmap/x-storable
Publisher: FIHMC CmapTools 6.04
Width: 2494
Height: 615
Type on Encryption
Random Numbers
vs Pseudorandom
not truly random
predictable
requirements
uniform distribution
independence
uses include
keys for public-key alg
stream key for symmetric stream cipher
session key
Message
Authenicates
aganst active attacks
verification of received message
messages can use conventional encryption
secure through
Hash Function
usage
fixed length output
h(x) easy to compute
applied to block data
how it's useful
Secuity
types of attack
brute force
cryptanalystic
type of alg used
SHA
application
intrusion detection software
passwords
Symetric
Algorithm
DES
characteristics
most studied
64 bit
most widely used
Triple DES
characteristics
repeats DES 3 times
112 or 168 bit
can be sluggish
AES
characteristics
128/192/256 bit
replaced 3DES
cyphers
stream
characteristics
produce output one at a time
fast and uses less code
process input continueously
encrypts plain text
block
characteristics
reuse keys
produce output block for every input
process input one at time
requiremens to be safe
Secure use
need
strong alg
sender and receiver must be secure
trype of attacks
brute force
done by
trying all possible keys
Cryptanalytic
relys on
nature of algorithm
knowlegde of plaintext
Asymmetric
types
ECC
RSA
Digital signature
Diffie Hellman
Public Key
structured by
public
types of applications
Digital Envelopes
requirements
exchanging keys beforesending and receiving msg
Digital signature
characteristics
created by hash code
used for source and data intergrity
doesn't provide confidentiality
Certificates
Characteristics
infeseasible for opponent to crack key
key can be used for either role
easy to create key
easy to create key pairs
private
uses
own key
data security