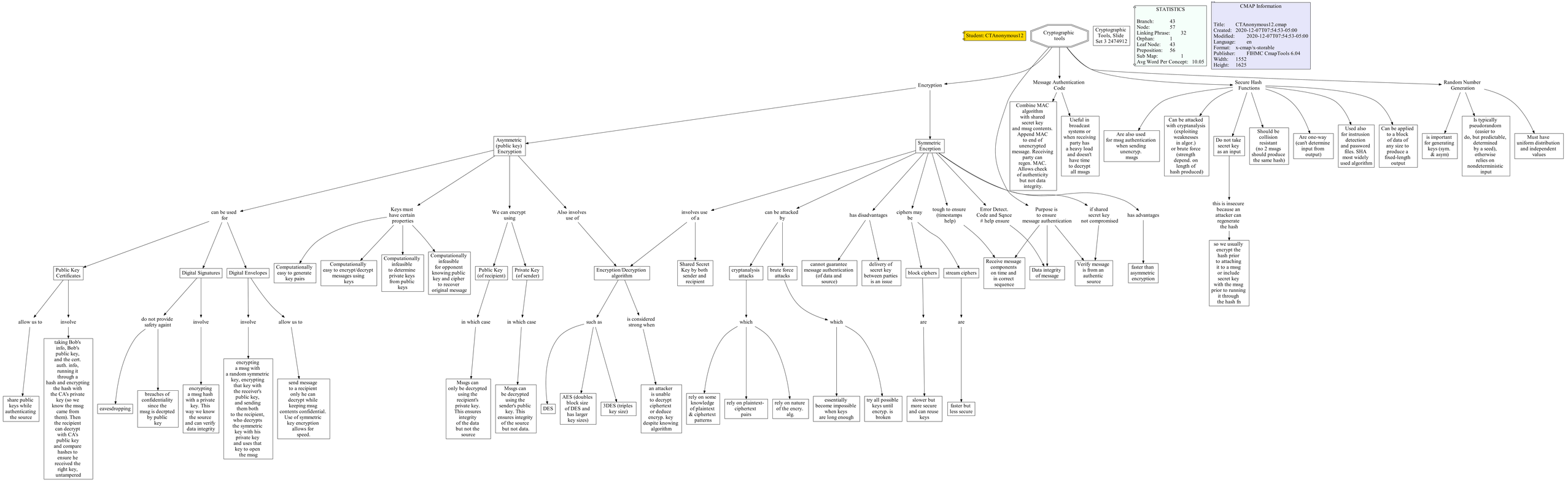
Student: CTAnonymous12
Cryptographic tools
Cryptographic Tools, Slide Set 3 2474912
STATISTICS
Branch: 43
Node: 57
Linking Phrase: 32
Orphan: 1
Leaf Node: 43
Preposition: 56
Sub Map: 1
Avg Word Per Concept: 10.05
CMAP Information
Title: CTAnonymous12.cmap
Created: 2020-12-07T07:54:53-05:00
Modified: 2020-12-07T07:54:53-05:00
Language: en
Format: x-cmap/x-storable
Publisher: FIHMC CmapTools 6.04
Width: 1552
Height: 1625
Encryption
Message Authentication Code
Secure Hash Functions
Random Number Generation
Combine MAC algorithm with shared secret key and msg contents. Append MAC to end of unencrypted message. Receiving party can regen. MAC. Allows check of authenticity but not data integrity.
Useful in broadcast systems or when receiving party has a heavy load and doesn't have time to decrypt all msgs
Are also used for mssg authentication when sending unencryp. mssgs
Can be attacked with cryptanalysis (exploiting weaknesses in algor.) or brute force (strength depend. on length of hash produced)
Do not take secret key as an input
this is insecure because an attacker can regenerate the hash
so we usually encrypt the hash prior to attaching it to a mssg or include secret key with the mssg prior to running it through the hash fn
Should be collision resistant (no 2 mssgs should produce the same hash)
Are one-way (can't determine input from output)
Used also for instrusion detection and password files. SHA most widely used algorithm
Can be applied to a block of data of any size to produce a fixed-length output
is important for generating keys (sym. & asym)
Is typically pseudorandom (easier to do, but predictable, determined by a seed), otherwise relies on nondeterministic input
Must have uniform distribution and independent values
Asymmetric (public key) Encryption
Symmetric Encrption
can be used for
Keys must have certain properties
We can encrypt using
Also involves use of
involves use of a
can be attacked by
has disadvantages
ciphers may be
tough to ensure (timestamps help)
Error Detect. Code and Sqnce # help ensure
Purpose is to ensure message authentication
if shared secret key not compromised
has advantages
Public Key Certificates
Digital Signatures
Digital Envelopes
Computationally easy to generate key pairs
Computationally easy to encrypt/decrypt messages using keys
Computationally infeasible to determine private keys from public keys
Computationally infeasible for opponent knowing public key and cipher to recover original message
Public Key (of recipient)
Private Key (of sender)
Encryption/Decryption algorithm
Shared Secret Key by both sender and recipient
cryptanalysis attacks
brute force attacks
cannot guarantee message authentication (of data and source)
delivery of secret key between parties is an issue
block ciphers
stream ciphers
Receive message components on time and in correct sequence
Data integrity of message
Verify message is from an authentic source
faster than asymmetric encryption
allow us to
involve
do not provide safety against
involve
involve
allow us to
in which case
in which case
such as
is considered strong when
which
which
are
are
share public keys while authenticating the source
taking Bob's info, Bob's public key, and the cert. auth. info, running it through a hash and encrypting the hash with the CA's private key (so we know the mssg came from them). Then the recipient can decrypt with CA's public key and compare hashes to ensure he received the right key, untampered
eavesdropping
breaches of confidentiality since the mssg is decrpted by public key
encrypting a mssg hash with a private key. This way we know the source and can verify data integrity
encrypting a mssg with a random symmetric key, encrypting that key with the receiver's public key, and sending them both to the recipient, who decrypts the symmetric key with his private key and uses that key to open the mssg
send message to a recipient only he can decrypt while keeping mssg contents confidential. Use of symmetric key encryption allows for speed.
Mssgs can only be decrypted using the recipient's private key. This ensures integrity of the data but not the source
Mssgs can be decrypted using the sender's public key. This ensures integrity of the source but not data.
DES
AES (doubles block size of DES and has larger key sizes)
3DES (triples key size)
an attacker is unable to decrypt ciphertext or deduce encryp. key despite knowing algorithm
rely on some knowledge of plaintext & ciphertext patterns
rely on plaintext-ciphertext pairs
rely on nature of the encry. alg.
essentially become impossible when keys are long enough
try all possible keys until encryp. is broken
slower but more secure and can reuse keys
faster but less secure