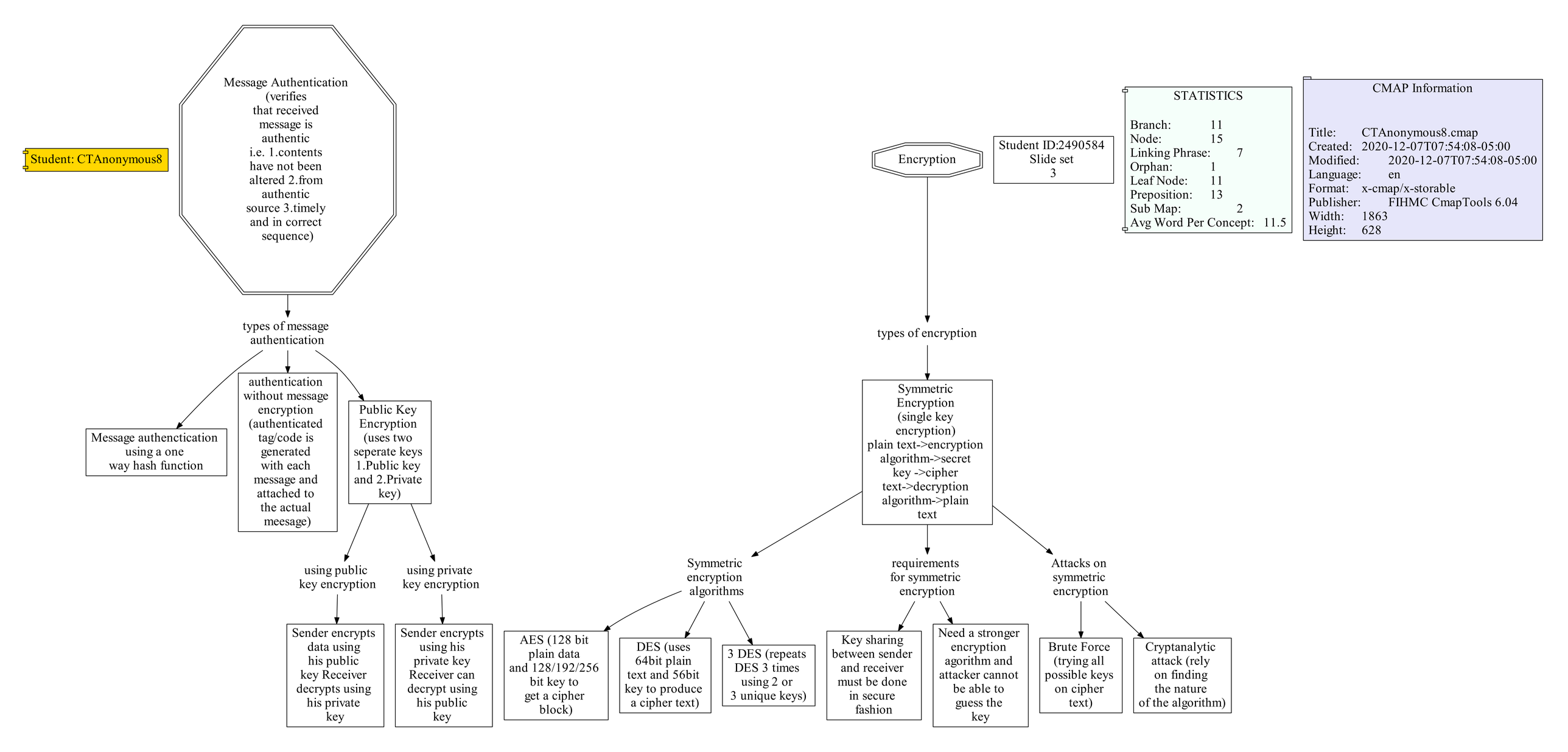
Student: CTAnonymous8
Message Authentication (verifies that received message is authentic i.e. 1.contents have not been altered 2.from authentic source 3.timely and in correct sequence)
types of message authentication
Message authenctication using a one way hash function
authentication without message encryption (authenticated tag/code is generated with each message and attached to the actual meesage)
Public Key Encryption (uses two seperate keys 1.Public key and 2.Private key)
using public key encryption
using private key encryption
Sender encrypts data using his public key Receiver decrypts using his private key
Sender encrypts using his private key Receiver can decrypt using his public key
Encryption
Student ID:2490584 Slide set 3
STATISTICS
Branch: 11
Node: 15
Linking Phrase: 7
Orphan: 1
Leaf Node: 11
Preposition: 13
Sub Map: 2
Avg Word Per Concept: 11.5
CMAP Information
Title: CTAnonymous8.cmap
Created: 2020-12-07T07:54:08-05:00
Modified: 2020-12-07T07:54:08-05:00
Language: en
Format: x-cmap/x-storable
Publisher: FIHMC CmapTools 6.04
Width: 1863
Height: 628
types of encryption
Symmetric Encryption (single key encryption) plain text->encryption algorithm->secret key ->cipher text->decryption algorithm->plain text
Symmetric encryption algorithms
requirements for symmetric encryption
Attacks on symmetric encryption
AES (128 bit plain data and 128/192/256 bit key to get a cipher block)
DES (uses 64bit plain text and 56bit key to produce a cipher text)
3 DES (repeats DES 3 times using 2 or 3 unique keys)
Key sharing between sender and receiver must be done in secure fashion
Need a stronger encryption agorithm and attacker cannot be able to guess the key
Brute Force (trying all possible keys on cipher text)
Cryptanalytic attack (rely on finding the nature of the algorithm)