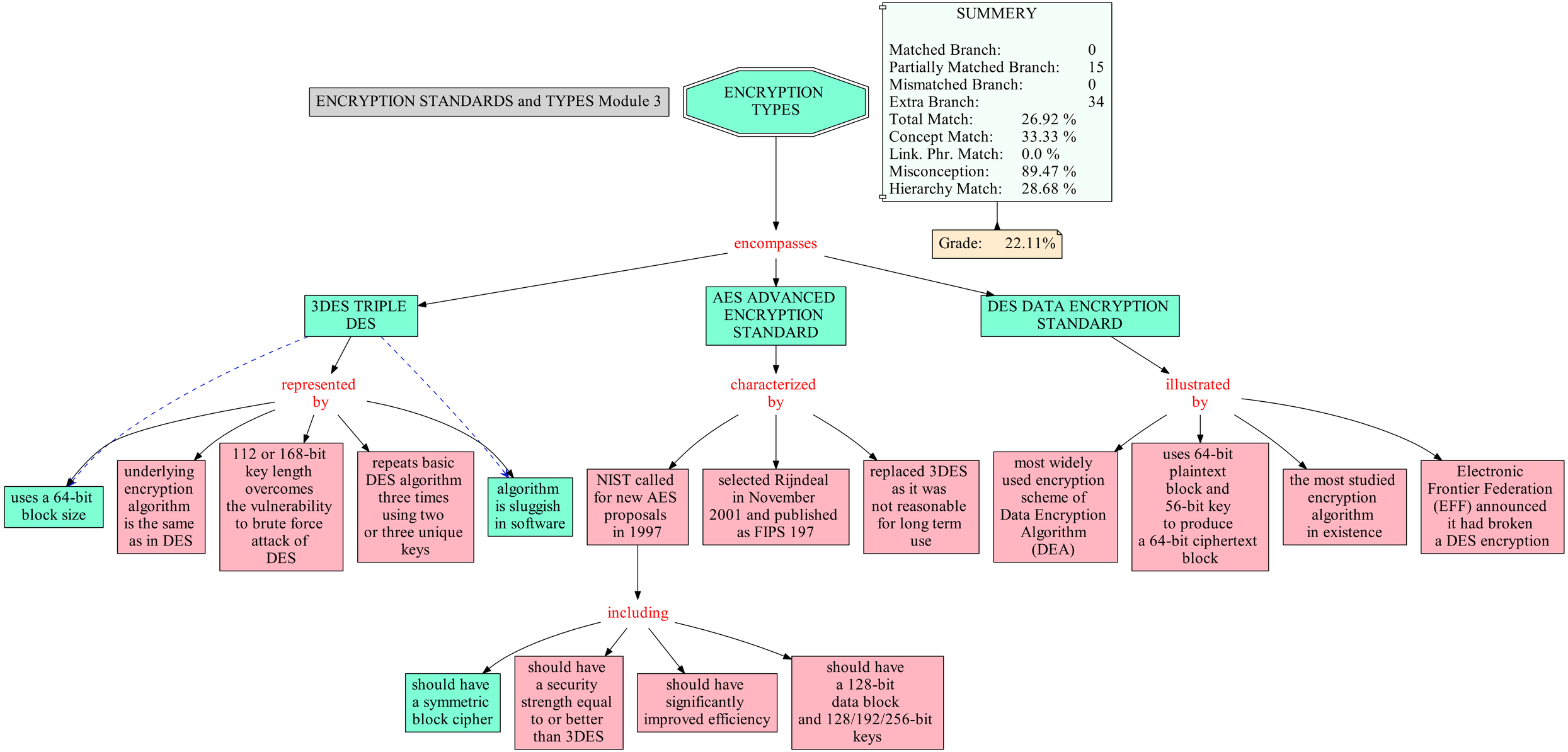
ENCRYPTION STANDARDS and TYPES Module 3
ENCRYPTION TYPES
SUMMERY
Matched Branch: 0
Partially Matched Branch: 15
Mismatched Branch: 0
Extra Branch: 34
Total Match: 26.92 %
Concept Match: 33.33 %
Link. Phr. Match: 0.0 %
Misconception: 89.47 %
Hierarchy Match: 28.68 %
Grade: 22.11%
encompasses
3DES TRIPLE DES
AES ADVANCED ENCRYPTION STANDARD
DES DATA ENCRYPTION STANDARD
represented by
characterized by
illustrated by
uses a 64-bit block size
underlying encryption algorithm is the same as in DES
112 or 168-bit key length overcomes the vulnerability to brute force attack of DES
repeats basic DES algorithm three times using two or three unique keys
algorithm is sluggish in software
NIST called for new AES proposals in 1997
selected Rijndeal in November 2001 and published as FIPS 197
replaced 3DES as it was not reasonable for long term use
most widely used encryption scheme of Data Encryption Algorithm (DEA)
uses 64-bit plaintext block and 56-bit key to produce a 64-bit ciphertext block
the most studied encryption algorithm in existence
Electronic Frontier Federation (EFF) announced it had broken a DES encryption
including
should have a symmetric block cipher
should have a security strength equal to or better than 3DES
should have significantly improved efficiency
should have a 128-bit data block and 128/192/256-bit keys