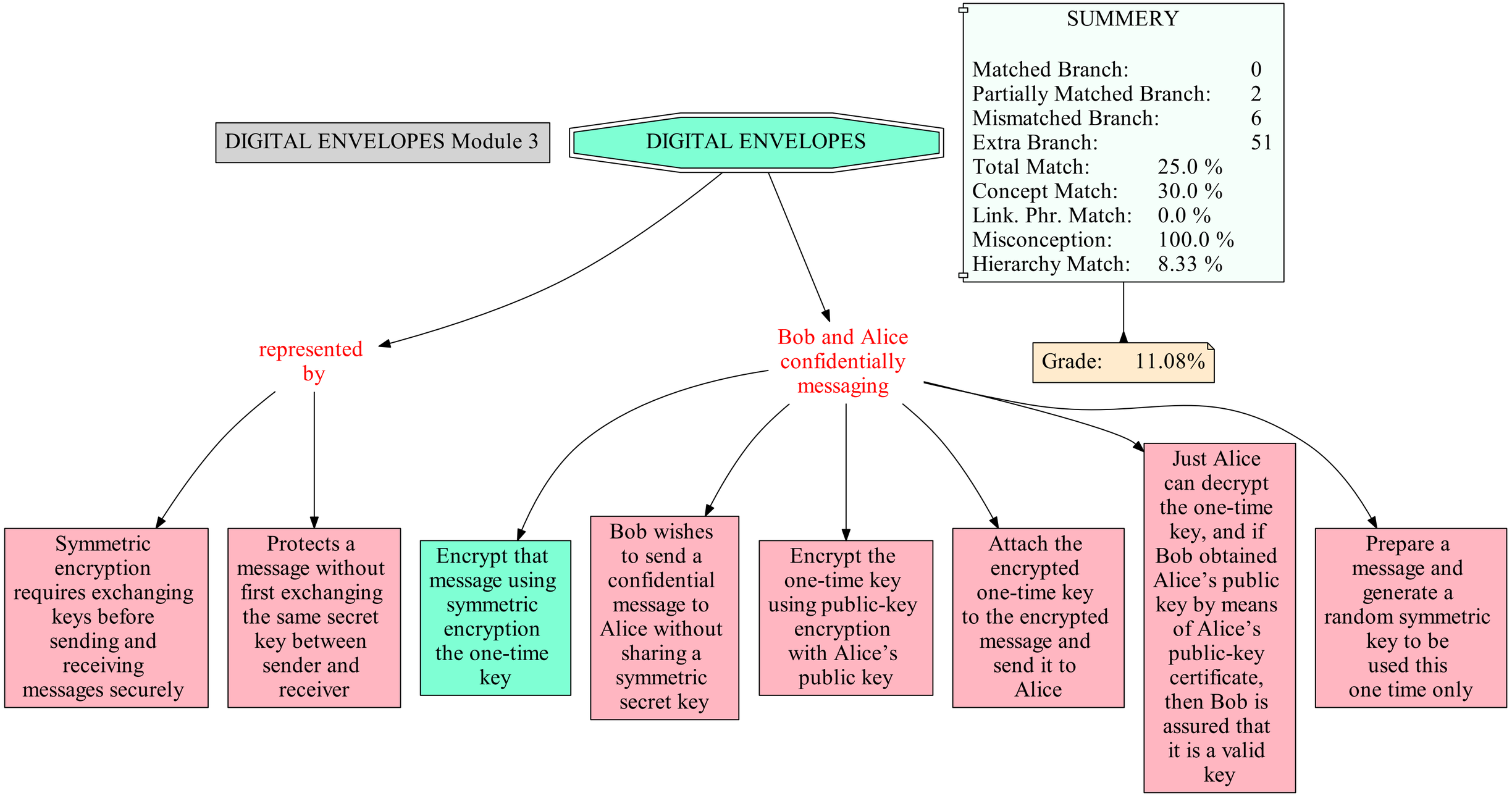
DIGITAL ENVELOPES Module 3
DIGITAL ENVELOPES
SUMMERY
Matched Branch: 0
Partially Matched Branch: 2
Mismatched Branch: 6
Extra Branch: 51
Total Match: 25.0 %
Concept Match: 30.0 %
Link. Phr. Match: 0.0 %
Misconception: 100.0 %
Hierarchy Match: 8.33 %
Grade: 11.08%
represented by
Bob and Alice confidentially messaging
Symmetric encryption requires exchanging keys before sending and receiving messages securely
Protects a message without first exchanging the same secret key between sender and receiver
Encrypt that message using symmetric encryption the one-time key
Bob wishes to send a confidential message to Alice without sharing a symmetric secret key
Encrypt the one-time key using public-key encryption with Alice's public key
Attach the encrypted one-time key to the encrypted message and send it to Alice
Just Alice can decrypt the one-time key, and if Bob obtained Alice's public key by means of Alice's public-key certificate, then Bob is assured that it is a valid key
Prepare a message and generate a random symmetric key to be used this one time only