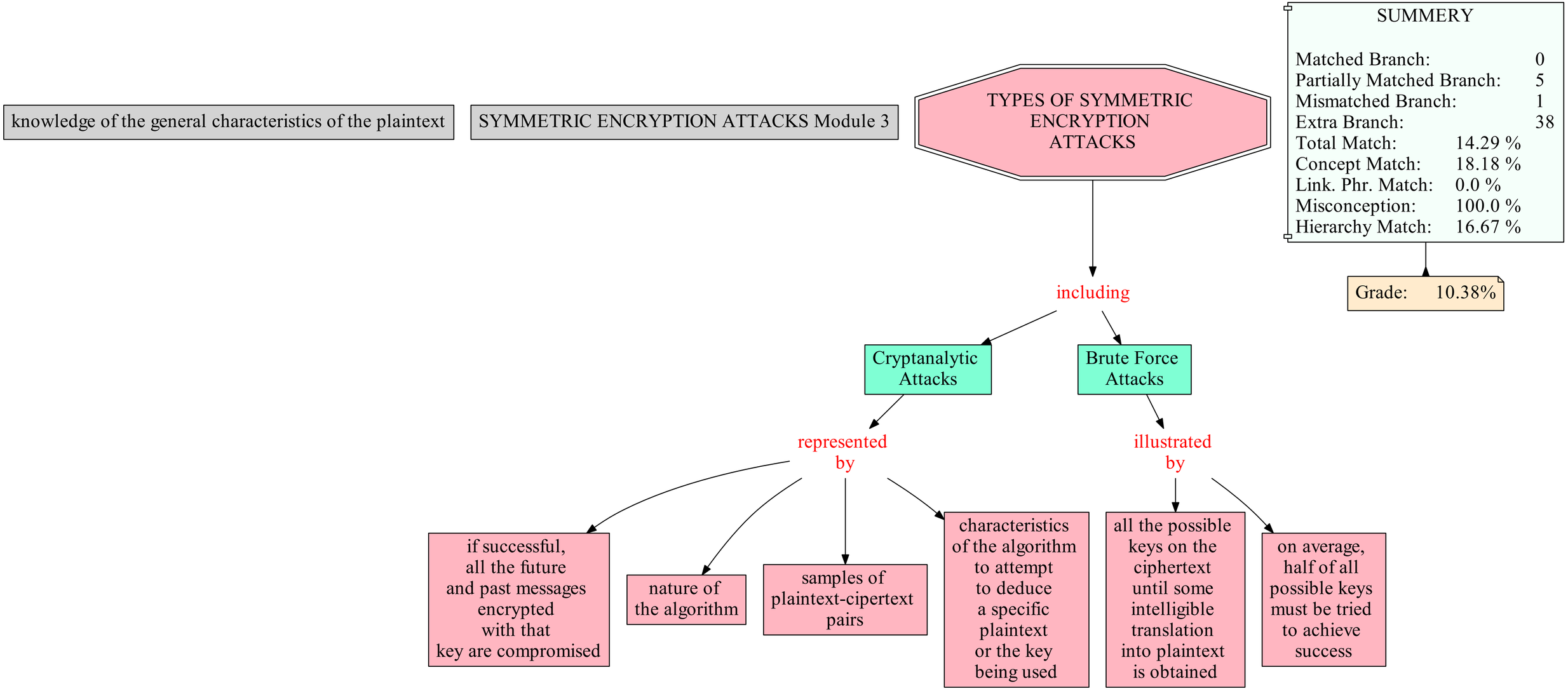
knowledge of the general characteristics of the plaintext
SYMMETRIC ENCRYPTION ATTACKS Module 3
TYPES OF SYMMETRIC ENCRYPTION ATTACKS
SUMMERY
Matched Branch: 0
Partially Matched Branch: 5
Mismatched Branch: 1
Extra Branch: 38
Total Match: 14.29 %
Concept Match: 18.18 %
Link. Phr. Match: 0.0 %
Misconception: 100.0 %
Hierarchy Match: 16.67 %
Grade: 10.38%
including
Cryptanalytic Attacks
Brute Force Attacks
represented by
illustrated by
if successful, all the future and past messages encrypted with that key are compromised
nature of the algorithm
samples of plaintext-cipertext pairs
characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
all the possible keys on the ciphertext until some intelligible translation into plaintext is obtained
on average, half of all possible keys must be tried to achieve success