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: 6
Mismatched Branch: 0
Extra Branch: 34
Total Match: 21.43 %
Concept Match: 27.27 %
Link. Phr. Match: 0.0 %
Misconception: 62.5 %
Hierarchy Match: 46.67 %

Grade: 35.31%

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