

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:	108
Total Match:	57.14 %
Concept Match:	54.55 %
Link. Phr. Match:	66.67 %
Misconception:	37.5 %
Hierarchy Match:	55.56 %

Grade: 58.37%

including

Cryptanalytic  
Attacks

Brute Force  
Attacks

represented  
by

illustrated  
by

nature of  
the algorithm

samples of  
plaintext-ciphertext  
pairs

characteristics  
of the algorithm  
to attempt  
to deduce  
a specific  
plaintext  
or the key  
being used

if successful,  
all the future  
and past messages  
encrypted  
with that  
key are compromised

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