

knowledge of the general characteristics of the plaintext

SYMMETRIC ENCRYPTION ATTACKS Module 3

TYPES OF SYMMETRIC
ENCRYPTION
ATTACKS

SUMMARY	
Matched Branch:	0
Partially Matched Branch:	6
Mismatched Branch:	0
Extra Branch:	47
Total Match:	28.57 %
Concept Match:	36.36 %
Link. Phr. Match:	0.0 %
Misconception:	87.5 %
Hierarchy Match:	47.78 %

Grade: 29.8%

including

Cryptanalytic
Attacks

Brute Force
Attacks

represented
by

illustrated
by

nature of
the algorithm

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

samples of
plaintext-ciphertext
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