13.09.18

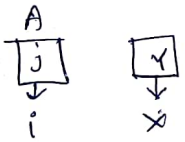
1

1.1 সব সব।
1.4 → Security service (list). Computer system security service.
Attack surface.
A Model for network security

2

2.1 Cryptanalysis vs Brute force.
Table. Simplified cipher model
Substitution cipher → ceaser, monoalphabetic.
One time pad → random. (publicly secure) (কারণ brute force দিয়ে ভাঙ্গতে পারবে না)
transposition.

One সব রকমের possible



Steganography

4

stream block cipher
Confusion, diffusion কোন use করা হয়।
DES, SDES (pdf).

5

6

AES এর structure এর structure.
transformation funct এর
6.4. key expansion Algorithm.
Avalanche effect.

7

Double DES, problem কি?
Triple " , এর password
এর "

1—7 → 3টা set } A বাকি-B
8—9 →

৯ম Mode table 7.1 কোথায় use হয়।
কিভাবে কাজ করে,

8

RNG Use of random no কি কোথায় দরকার,
কখন বলব " "

TRNG

PRNG Requirement

8.4 Stream cipher def, কখন use হয়।
RC4 কি ? description.

9

RSA idea.
" requirement.
Conventional vs public-key
RSA description + calculation.

10 বাদ

Set-A

1. Feistal structure used in → DES, SDES.
2.
3. Cryptanalysis is used to - find a better soln
4. In asymmetric key cryptography, the pri key is kept by - sender
5. RC4 is - Random no generator, stream cipher
6. A digital signature is - easy to produce
7. Kerberos v4 uses - DES
8. How many round keys are generated in the AES algorithm - 10, 12, 14
9. No of key used in 3DES is → 2, 3
10. Hash func का use → encryption.

set-B.

11

Hash

11.1 Application

MAC → use, definition

11.3 Req and security

Table 11.1 Attack Brute force attack

Preimage

Collision resistant u

Cryptanalysis

SHA-512 এর description.

12 Msg Authen Code

Requirment

Msg Authen functn

Uses MAF

MAC → Msg Auth. Code

MAC

Requirements

Security of MAC

HMAC → Algo.

Security of HMAC

12.9 PRNG based on Hash func.

Hash কারি যদি ওরকম no হয় generally random no হবে।

Digital signature কি? কেন use করি?

DSA খুবগুরুত্ব

14

14.1 KDC idea

Session key lifetime.

14.2 Sym key dis using asym key
See " " with confidentiality

14.3 Distribution of

15

Mutual authentication 475 page
User " ~~fo~~
Timestamp ~~fo~~
Kerberos
" 4 vs K-5

~~16~~ 18

Email Protocols
SMTP
MIME ~~কি~~ ~~চিঠি~~ ? Binary data পাঠানো যায় ।
SMIME ~~কিভাবে~~ Security provide করে ।