original

Tentamen Nätverkssäkerhet DAVC23

40p + 20p lab = 60p

Hjälpmedel: inga

7 juni 2006 8:15 – 13:15

Ansvarig lärare	Rum	Ankn.
Thijs Holleboom	5A412	1148
Simone Fischer-Hübner	5A435	1723

Poäng	Betyg
40–46	3
47–53	4
54–60	5

1 Begrepp (3p)

Redogör kortfattat för innebörd och funktion av följande begrepp:

a. unconditionally secure encryption scheme

b. computationally secure encryption scheme

c. brute force attack

d. polyalphabetic substitution cipher

e. transposition cipher

f. pseudo random number

2 Nyckeldistribuering (5p)

Motivera alla dina svar!

a. (1p) Hur många nycklar behövs om N endpoints (hosts) ska kunna kommunicera på ett säkert sätt och använder symmetrisk kryptering.

b. (1p) Om ovannämnda hostar väljer att i stället använda asymmetrisk kryptering, hur många privata och publika nyclar behövs då?

c. (1p) Hur många nycklar behövs minst i fall ovannämnda hostar använder sig av ett key distribution center och använder symmetrisk kryptering.

d. (1p) Beskriv hur asymmetrisk kryptering löser nyckeldistribueringsproblemet

e. (1p) Beskriv hur RSA algorithmen för asymmetrisk kryptering fungerar.

3 DES (7p)

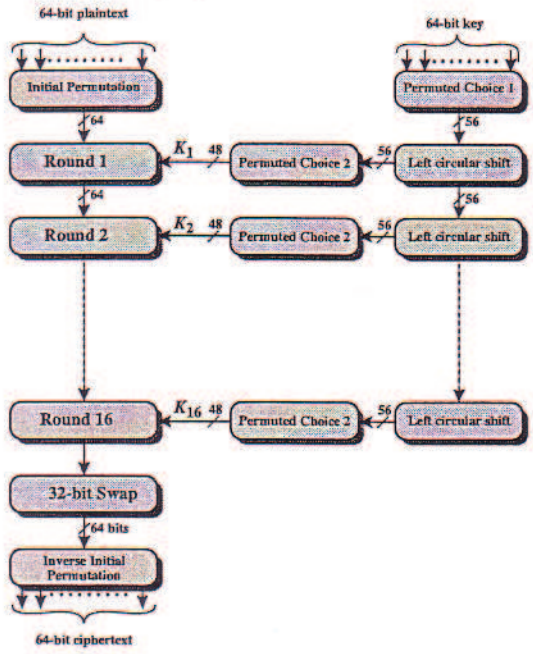

Figure 3.4 General Depiction of DES Encryption Algorithm

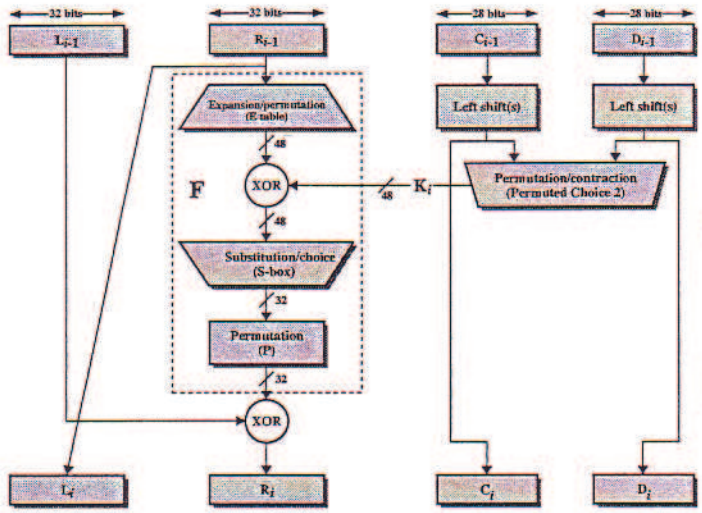

Figure 3.5 Single Round of DES Algorithm

DES krypteringsalgoritmen kan översiktligt beskrivas med hjälp av ovanstående två figurer, 3.4 och 3.5, som är hämtade från kursboken (Stallings, *Cryptography and network security*).

a. (2p) DES algoritmen har en så kallad Feistelstruktur. Vilka två koncepter ligger till grund för Feistelstrukturens kryptografiska styrka. Beskriv vad dessa koncepter innebär och hur de fungerar i Feistel strukturen.

b. (2p) Beskriv DES algoritmen med hjälp av ovanstående figurer, beskriv vad de olika komponenter i figurerna står för och vad de gör.

c. (1p) $\bar{X}$ betecknar bitvis komplement av X. Visa att $\overline{A \oplus B} = \bar{A} \oplus \bar{B}$.

d. (2p) Visa att om C är resultatet av att kryptera texten M med nyckel K då fås $\bar{C}$ om $\bar{M}$ krypteras med $\bar{K}$.

e. Hur påverkas säkerhetn av DES alhoritmen av resultatet ovan.

4 Diffie-Hellman (5p)

Diffie-Hellmanm protokollet för utbyte av nycklar innefattar två globala parametrar, ett primtal q och ett tal α som är en primitiv rot av q och uppfyller $q < \alpha$.

a. (2p) Beskriv i detalj hur två parter, A och B, kan byta ut en hemlig nyckel K. Varje part genererar två tal, X_A och Y_A, respektive X_B och Y_B, där endast A känner till X_A och endast B känner till X_B. Beskriv vilka matematiska operationer som ingår och hur man kan garantera att K är hemlig.

b. (2p) Beskriv i detalj hur en *man in the middle attack* på ovannämnda protokollet går till.

c. (1p) Hur kan man gardera sig mot ovannämnda *man in the middle attack*?

5 Block Cipher Modes (5p)

a. (1p) Beskriv vad som är, kryptografiskt sett, svagheten med Electronic Code Book Mode of operation om datamängden som krypteras består av flera block.

b. (1p) Beskriv hur Cipher Block Chaining Mode åtgärdar ovanstående svagheten.

c. (3p) Beskriv *i detalj* hur cipher Feedback Mode fungerar och hur det kan användas till att konvertera ett block chiffer till ett stream chiffer.

6 Autentisering, signaturer och hashfunktioner (5p)

I kursboken nämns 6 krav som ställs på hashfunktioner $H(x)$, där de första tre är

i) Godtycklig storlek på x

ii) Fast storlek på H

iii) $H(x)$ beräknas effektivt.

a. (2p) Beskriv de övriga tre krav, vad de innebär och varför de finns.

b. (3p) Beskriv översiktligt, med hjälp av diagram, hur hashfunktioner används för att åstadkomma följande:

i) (1p) Autentisering av ett meddelande M m.h.a. $H(x)$ och symmetrisk kryptering.

ii) (1p) Autentisering och signatur av ett meddelande M m.h.a. $H(x)$ och publik nyckel kryptering.

iii) (1p) Autentisering, signatur och kryptering av ett eddelande M m.h.a. $H(x)$ och publik nyckel kryptering.

7 IPsec (3p)

a. (1p) Jämför link-encryption och end-to-end encryption och ange för- och nackdelar med båda.

b. (2p) Beskriv översiktligt hur IP security (IPSec) fungerar och beskriv i detalj vilka tjänster (services) IPSec erbjuder och hur IP-paket headrar modifieras (endast IPv4). Din beskrivning ska bland annat täcka transport och tunnel mode, security association och sequence number counter.

8 PET (7p)

Besvara denna uppgift på ett separat papper!

Explain the functionality and privacy protection properties of

a. (4p) Mix nets

b. (3p) Crowds