Tentamen i Säkerhet (EDA625)

130403 8.00-13.00

Tillåtna hjälpmedel: Miniräknare

Maxpoängen för provet är totalt 60 poäng. För betyget 3 krävs minst 30 poäng som får vara fördelade godtyckligt mellan uppgifterna. Lycka till !

1. Förklara kort begreppen: (1) Blockchiffer, (2) Strömchiffer, (3) CBC-mode, (4) Birthday paradox, (5) Öpen-nyckel kryptosystem, (6) hashfunktion och (7) MAC-funktion. (10p)
.

Ledning: se kursmaterial. 5: viktig att man beskriver privat och publik nyckel. 7: glöm inte att nämna att man använder en delad hemlig nyckel.

2. RSA-kryptering är grunden till många olika kryptosystem. När man bestämmer ett RSA-system så väljar man två primtal p och q. Låt p=149 och q=157. Den publika exponenten kan vara e_1=195 eller e_2=209. (OBS e_1 och e_2 är inte primtal!)

a) Bestäm (beräkna) vilken av e_1 och e_2 som fungerar tillsammans med RSA (3 p)
b) Använd svaret på a) för att bestämma den hemliga exponenten d (4 p)
c) Kryptera meddelandet m=3 (3 p)

Svar: a) 209 fungerar b) d=19553 (-3535 godtages också) c) 13695

3. Hashfunktioner har en viktig roll vid digital signering av data.

a) Ge en kort förklaring varför hashfunktioner används. Texten ska innehålla minst två motiveringar. (2p)
b) Födelsedagsparadoxen kan användas som ett instrument för att ge en undre gräns på sannolikheten att någon lyckas att skapa en falsk signatur. Förklara varför det är så. (5p)
c) Födelsedagsparadoxen anger att när man väljer N bollar som man stoppar slummässigt en efter en i K stycken olika lådor att sannolikheten att två bollar hamnar i samma låda är $P(N,K)\approx 1-\exp(-N^2/(2K))$. Beräkna antalet olika meddelanden du slumpmässigt kan skapa tills sannolikheten att en kollision av meddelandens hashvärden är 1-(1/e). Anta att din hashfunktion producerar ett hash-värde som är 256 bitar lång. (3p)

Ledning: a) själva signeringsalgoritmen kan inte hantera stora data mängder på ett effektivt sätt så det är mer effektivt att först ta hash värdet på data. Ger redundans bryter den multiplikativa strukturen i RSA. b) Födelsedagparadoxen ger undre gräns på sannolikheten på en hashkollision. Sedan kan man koppla sådan hashkollisioner till att lyckas med att skapa en falsk signatur. c) $\text{sqrt}(2^{257})$

VAR GOD VÄND

4. Accesskontrollen i ett datorsystem kan implementeras på olika sätt. MAC och DAC är två olika typer av accesskontroll som ofta används.

a) Namnge ett operativ system där DAC resp MAC används. (2p)

b) Beskriv principen för ett DAC resp MAC accesskontroll och ge två exempel där ett DAC resp MAC baserat system är att föredra (5p)

c) Ett tredje system betecknas som RBAC. Beskriv skillnaden mellan RBAC och DAC? (3p)

Ledning: a) DAC: windows, linux, MAC: SELinux. b) se kursmaterial. DAC är att föredra i eget desktop PC system. MAC i datorsystem för att regelstyrd verksamhet med höga krav på skydd. c) se kursmaterial.

5. Att skydda en dataförbindelse kan göras med hjälp av TLS eller IPsec.

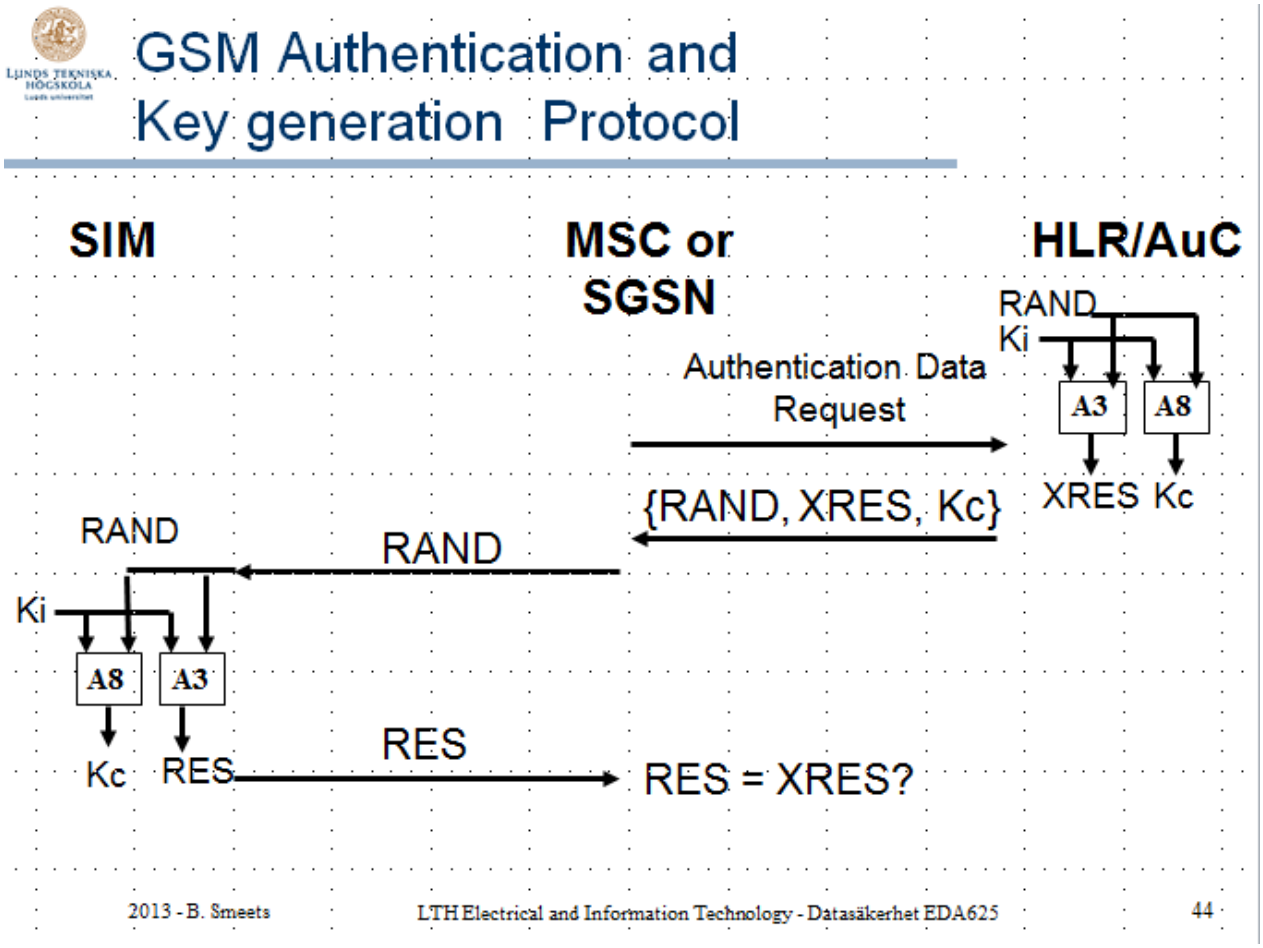
a) Förklara hur sessions-nyckeletableringen sker i TLS resp IPsec. (2p)
b) Förklara hur användardata (dvs nyttodata) skyddas av TLS resp IPsec i termer av vilken skydd som erbjuds. (2p)
c) Förklara i vilket fall IPsec är att föredra över TLS. (3p)
d) Förklara hur en VPN tunnel fungerar och varför den kan användas utomlands för att titta på svtplay program som normallt inte går att spela upp utomlands. (3p)

Ledning: a) se kursmaterial. Komm igåg att IPsec få sina nycklar utifrån. b) TLS och IPsec kan erbjuda: kryptering, integritet och skydd mot replay. Man ska beskriva att TLS och IPsec har olika moder som styr vilket skydd är påslagen och vilka algoritmer som används. Se kursmaterial. Glöm inte IPsec tunnelmode. c) när skyddet måste ske på IP nivå. d) se kursmaterial. Glöm inte beskriva hur IP adress hanteringen görs för att ge intryck att du befinner dig i Sverige.

6. Bilden nedan kommer från lektionsföreläsningen och föreställer autentisering och kryptonyckelberäkningen i ett GSM system.

a) Använd bilden för att förklara i ord hur autentiseringen går till i GSM. (5p)
b) I UMTS systemet (3G) har man löst ett allvarligt problem med GSM autentiseringen. Beskriv detta problem och lösningsprincipen i UMTS. (3p)
c) Om vi antar att kryptot som används inte kan forceras (knäckas) hur kan man då avlyssna (med myndigheters tillstånd) ett samtal i ett GSM resp i ett 3G system. (2p)

Ledning: a) förklara i ord det som bilden visar, se kursmaterial. b) falsk basstation, ömsesidig (mutal) autentisering med hjälp av räknare och mac skydd på challenge. c) beskriv hur operatören vet kryptonycklarna, var de används och hur de kan brukas av den som ska avlyssna. Nämn också att om man nöjer sig med att avlyssna bakom basstationen då är trafiken i princip okrypterad så man behöver bara operatörens hjälp att komma in i hans nätverksnoder. Nämn också att i 3G termineras krypto ett steg djupare i infrastrukturen, i RNC noden (man behöver dock inte veta namnet på denna nod för att få godkänd).


GSM Authentication and
Key generation Protocol
SIM
MSC or
SGSN
HLR/AuC
RAND
Ki
A3
A8
XRES Kc
Authentication Data
Request
{RAND, XRES, Kc}
RAND
RAND
Ki
A8
A3
Kc
RES
RES
RES = XRES?
2013 - B. Smeets
LTH Electrical and Information Technology - Datasäkerhet EDA625
44

LYCKA TILL!