Tentamen i Säkerhet (EITF55, EDA625)

180830 8.00-13.00

- Svara på svenska eller engelska.
- Tillåtna hjälpmedel: miniräknare.
- Om du saknar någon information, gör rimliga antaganden. Skriv då också ner vilka antaganden du har gjort.
- Skriv läsligt. Om något svar är oläsligt så får du inga poäng på den uppgiften.
- För betyg 3 krävs minst 30 poäng, som får vara godtyckligt fördelade mellan uppgifterna. Varje uppgift kan ge 10 poäng. Maxpoängen för provet är totalt 60 poäng. Betygsättning enligt nedan.
  Betyg 3 = 30 -- 39 poäng,
  Betyg 4 = 40 -- 49 poäng,
  Betyg 5 = 50 -- 60 poäng.

1. a) Förklara skillnaden mellan MAC och hash algoritmerna. (2p)
   b) Förklara hur Diffie-Hellman algoritmen kan användas för att skapa en krypterings nyckel mellan två parter. (2p)
   c) Förklara vad som menas med RBAC. (2p)
   d) Vad är speciellt med AEAD mode? (2p)
   e) Förklara vad är en PKI. (2p)

ej relativt primt med (p-1)(q-1)=50616

2. RSA-kryptering är grunden till många olika kryptosystem. När man dimensionerar ett RSA-system så väljer man två primtal, p och q. Låt p=223 och q=229 Den publika exponenten kan vara e_1=373 eller e_2=210.
   a) Bestäm (beräkna) vilken av e_1 och e_2 som fungerar tillsammans med p och q (3p)
   b) Använd svaret på a) för att bestämma den hemliga exponenten d (3p)
   (Ifall båda e_1 och e_2 fungerar så använd bara e_1 för att bestämma d!)
   c) Kryptera meddelandet m=482. (3p)

d1=1357

6960

OBS 1: Korrekt svar på deluppgift utan redovisad beräkning ger noll poäng.
OBS 2: Felaktigt svar med huvudsakligen korrekt beräkning ger minimalt avdrag.

3. Nedan hittar du ett antal påståenden om TLS och IPsec och svarsalternativ. Kryssa i tabellen på nästa sida för vilket svar som är korrekt. Du måste för minst fyra (4) påståenden ange om du är säker på att ditt svar är rätt om du vill nå fullt poängantal för denna uppgift. Svara genom att kopiera tabellen till ditt svarsblad och ange ditt svar i den kopierade tabellen. Felaktigt svar då du ange att du är säker ger 1 poäng-avdrag. Annars ger fel svar 0 poäng. Rätt svar ger 1 poäng och är du säker fås 2 poäng. Max poäng för hela uppgiften år 10 och minst 0p.
   a) IPsec AH kan användas för sekretess och integritetsskydd.
   b) IPsec ESP inkluderar inte nyckeletablering men det gör IPsec AH.
   c) IPsec AH och TLS kan kryptera data som överförs.
   d) Applikationer som använder säker kommunikation behöver modifieras om vi vill skydda dess datatrafiken med TLS.
   e) En VPN tunnel kan göras med DTLS
   f) TLS fungerar inte med symmetriska nycklar.

fel

fel

fel

rätt

rätt

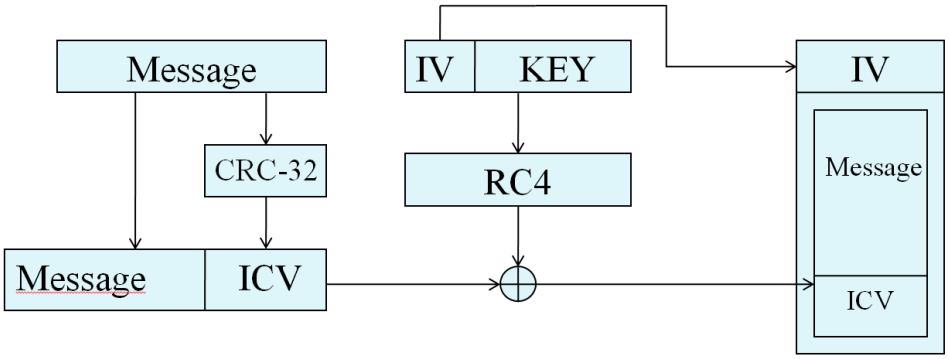
fel

Forts uppgift 3

Påstående	Stämmer Jag är säker	Stämmer	Stämmer inte	Stämmer inte Jag är säker
a)				
b)				
c)				
d)				
e)				
f)				

Täcks inte längre av kursboken

4. Betrakta följande illustration av krypteringsförfarandet i WEP. CRC-32 är en checksumma algoritm som beräknar integritets checksumma ICV.



WEP var designat för att ge konfidentialitet, integritet och autentisering. På grund av (extremt) dåliga designval så lyckades WEP dock inte nå något av dessa tre designmål.

a) Vilken sorts chiffer är RC4? (1p)
b) Visa att konfidentialiteten (krypteringen) i WEP är undermålig. (3p)
c) CRC-32 är en linjär funktion. Varför är detta dåligt? (4p)
d) Vad innebär Kerckhoff's princip? (2p)

Ledning till b): IV repeteras efter 2^{24} frames. Visa att två (olika) krypterade meddelanden med samma IV kan adderas (med xor) och därmed ge (viss) information om ursprungsmeddelandena.
Ledning till c): CRC-32 är en linjär funktion, dvs. CRC-32(x⊕y)=CRC-32(x) ⊕CRC-32(y). ⊕ = XOR addition. Vad betyder detta om du ändar, säg sista biten i, meddelande M?

5. Lisa jobbar på ett företag som gör övervakningskameror. Hon upptäcker att i den TLS lösning som används har man vald att använda AES-ECB och att man använder sig av TLS med en 512bit RSA nyckel i server och en 512 bit RSA nyckel i kameran som lagras i flashminne tillsammans med kamerans mjukvara och annan data.
Hjälp Lisa med att föreslå förbättringar nedan som hon anser bör göras. Förklara dina svar och ger argument som Lisa kan använda för att hennes chef Per anser det befogat att ägna tid(pengar) på förbättringar.

a) En bättre krypteringsmetod? (2p)
b) Är det något fel med valet av RSA nycklar? Förklara ditt svar. (2p)
c) Om vi bara behöver säkerställa säker mjukvara uppdatering av kamerans mjukvara vilka av de ovannämnda RSA nycklar behövs för att göra lösningen säkert. Motivera ditt svar! (2p)

d) Om man i TLS ska i stället använda sig av Diffie-Hellman vad behöver Lina tänka på in en sådan lösning? (2p)

e) Förklara varför Lina vill använda elliptisk kurva baserad krypto is stället för RSA som Per är bekant med. (2p)

6. Betrakta följande frågor.
   a) Vilka är de vanligaste orsakerna som bidrar till att säkerhetsincidenter inträffar och vilka är de vanligaste kategorierna av incidenter? (2,5p)

   b) Mänskliga misstag är oftast den största anledningen till incidenter. Ange de orsaker du känner till som kan leda till oavsiktliga händelser. (2,5p)

   c) Antag att ditt datasystem utsatts för en ”oönskad händelse” som kostat dig 15000kr. Du blir erbjuden att köpa ett skydd för 2000 kr per år som dels gör att motsvarande händelse bara skulle kosta 1000 kr och dels gör att motsvarande händelse förväntas inträffa fem gånger mer sällan. Vad behöver du ta hänsyn till för att bestämma om du skall köpa det erbjudna skyddet eller inte? (2,5p)

   d) Antag att du är säkerhetsansvarig för ett stort datasystem och får reda på följande: Användarna har upptäckt att om man har kommit in i systemet med hjälp av sitt eget lösenord så kan man fritt byta mellan identiteter inne i systemet och därmed både läsa och skriva i andras filer. Användarna verkar inte speciellt bekymrade eftersom de litar helt på varandra. Vad gör du lämpligen. (Beskriv lämpliga åtgärder i punktform och kronologiskt). (2.5p)

LYCKA TILL!