Tentamen i Säkerhet (EITF55, EDA625)
Med ledning till svaren

190321 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 digital signatur algoritmerna. (2p)
   b) Förklara hur RSA algoritmen kan användas i S/MIME för att skicka krypterade email till en part med känd publik nyckel. (2p)
   c) Förklara vad som menas med ABAC. (2p)
   d) Förklara skillnaden mellan ECB och CTR mode? (2p)
   e) Förklara vad är en MMU och dess säkerhets relevans. (2p)

   a) MAC använder symmetriskt krypto och därmed uppnås inte non-repudiation egenskapen som finns i dig sig som använder asymmetriskt krypto. b) se boken, RSA används för kryptering av symmetrisk krypto nyckel som används för att kryptera e-post data. c) se boken, d) se boken e) en MMU är en hårdvara enhet in i dator som hjälper att realisera virtuellt minne och att skydda minnesaccessen mellan olika användare.

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=233 Den publika exponenten kan vara e_1=225 eller e_2=205.
   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 (4p)
   (Ifall båda e_1 och e_2 fungerar så använd bara e_1 för att bestämma d!)
   c) Kryptera meddelandet m=391. (3p)

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

   a) e1 funkar inte, e2 ok b) d2=11557 c) c= 37117

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 ESP kan användas för sekretess och integritetsskydd.

b) IPsec ESP och AH integritets skyddar hela IP paket
c) IPSec inkluderar inte nyckeletablering men det gör TLS.
d) IPsec AH och TLS kan kryptera data som överförs.
e) Applikationer som använder säker kommunikation behöver modifieras om vi vill skydda dess datatrafiken med IPsec.
f) TLS använder samma nyckel för att kryptera ingående och utgående data.
a) ok b) fel c) ok d) fel e) fel f) ok

Forts uppgift 3

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

4. Betrakta följande problem. Alice kan läsa och skriva till filen U, läsa filen V och exekvera filen W. Bob kan läsa filen U, läsa och skriva till V och har ingen access till W. Charlie kan läsa filen U, har ingen access till filen V och läsa filen W.

a) Bestäm och skriv ner access kontrollista för denna situation. (3p)
b) Bestäm och skriv ner ”capability” lista för denna situation. (3p)
c) Vad är skillnaden mellan en accesskontrollista och en capability lista i termer av revokering av alla access rättigheter till en specifik fil och revokering av all accessrättigheter för en viss person? (4p)

a.) T.ex för varje av de 3 filer gör en länkad lista med beskrivningar vad varje person får göra med filen och referens till nästa beskrivning (för nästa person).
b.) T.ex för varje person gör en länkad lits med beskrivningar för varje fil vad denna person få göra med filen och om personen är ägaren
c.) används en accesskontrol lista är det lätt att revokera en specifik persons access till en specifik fil men det är svårare att revokera denna personen’s samtliga rättigheter eftersom de ligger spridda. Används capability lista så revokeras enkelt samtliga access rättigheter

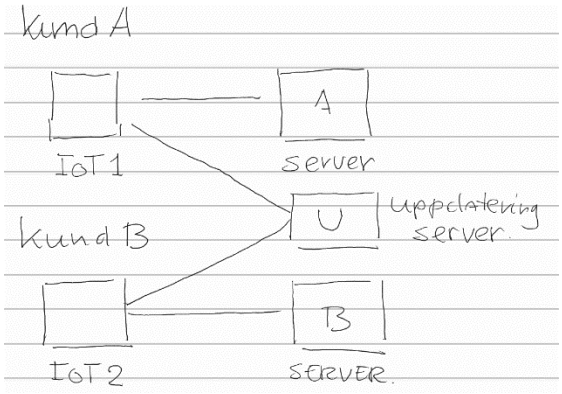
5. Aliya jobbar på ett företag som gör IoT styrenheter till kraftverk och ansvarar för enheternas säkerhetslösning. Kunderna kräver att hennes företag säkerställer att enheterna på ett säkert sätt koppla sig upp till kundernas serverar och att enheterna regelbunden uppdateras med senaste mjukvara från en server på Aliya’s företag. Kryptografiska nycklar som används ska vara RSA baserad eller för AES. Aliya ska lämna ett förslag till en systemlösning till hennes produktchef Åsa.

a) Rita en översiktsbild som visar ett system med två olika IoT enheter som ägs av respektive kund och Aliya’s företag och som visar data flöden mellan enheterna och kunderna (server) och uppdateringar. (2p)
b) Hjälp Aliya med att göra ett förslag hur IoT enheter kan koppla upp sig till kundernas servrar på ett säkert sätt och ger en förklaring som Aliya kan använda när hon argumenterar för sin lösning med Åsa. (3p)
c) Hjälp Aliya med att göra ett förslag hur IoT enheter kan uppdateras på ett säkert sätt

och ger en förklaring som Aliya kan använda när hon argumenterar för sin lösning med Åsa. (4p)

d) Aliya tycker att kundkravet att använda RSA är inte optimalt och vill istället använda elliptisk kurva baserad krypto (ECC). Vilka argument kan Aliya använda för att Åsa går med på att också implementera ECC stöd i enheterna? (1p)

a)



b) Varje IoT enhet får en egen nyckel och device certifikat från en CA och CAs root certifikat samt ett server certifikat till resp kund server och server certifikat till uppdaterings server U. Respektive server får en CA root certifikat för att verifiera IoT device certifikat och server nyckel och certifikat från samma CA. Sedan används TLS med ömsesidigt autentisering (dvs klient+server auth) som säkerställer att IoT kommunicera bara med betrodda servar, tex IoT1 med A resp U men inte med B. Vidare är genom TLS kommunikationen skyddat med kryptering, integritet och replay.

c) Vi installerar också en publik nyckel i varje IoT enhet som motsvarar en hemlig asymmetrisk krypto nyckel som används för att signera kod till IoT enheterna.

d) ECC behöver kortare nycklar för att uppnå samma säkerhet som RSA och därmed blir också meddelanden som skyddas med ECC kortare vilket gör ökat effektivitet.

6. Betrakta följande frågor för certifikat i en PKI.

a) Vad är en PKI och vad är rollen för en CA? Ger ett exempel på en PKI med minst fyra olika certifikat (se ledning). (4p)

b) Kan i två olika PKI uppsättningar finnas certifikat med samma publik nyckel? Förklara ditt svar. (1p)

c) Diffie-Hellman protokollet är i sin grundform inte säkert pga risken för en man-in-the-middle attack. Förklara varför. (2p)

d) Beskriv hur användandet av en PKI kan lösa problemet med risken för en man-in-the-middle attack. Ger en ritning/diagram hur meddelanden skickas mellan Alice och Bob som vill använda din förbättra protokoll. (3p)

Ledning: Du kan anta att vi använder RSA nycklar för certifikat och att ett certifikat har följande förenklade struktur specifikation:

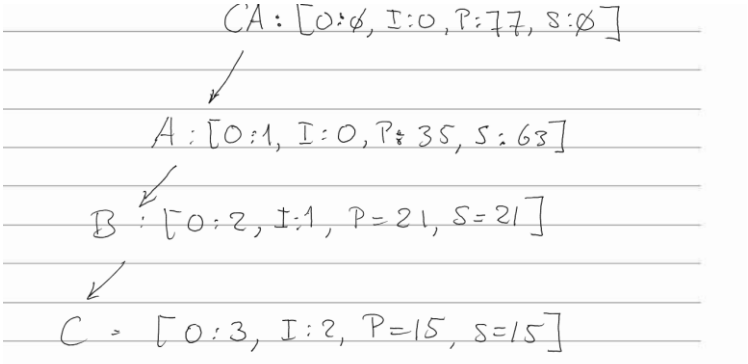
```
CERT[
  O: owner name,
  I: issuer name,
```

P: public key parameters (use for simplicity a numbers between 1 and 128),
S: issuer signature]

Lista med små primtal om det skulle behövas:

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113

a) Se boken för första delen
Sedan kan tex bygga ett PKI träd för en CA som är root i trädet och där varje nod tillhör tex en person som få ett löpnummer som namn och där publik exponent är alltid 7 och signaturen i certifikatet är signaturen av det resterande del av publika nyckel, dvs modulus talet n. CA här löpnummer 0.
För att det ska fungera med signering utan att införa en hash funktion måsta alla noder använda sig av ett modulus tal som är mindre än CAs eller issuer's publika modulus talet och vi accepterar att CAs self-signerat certifikat har signatur (värde) 0. Om man bygger trädet så ska man vara lite smart att se till att man håller moduli talen små för att minska arbetet. Det kan finnas många lösningar. Om din signatur lösning inte är korrekt får du 1p avdrag. Om du lämnar signature som $(n_{owner})^{d_{issuer}} \bmod n_{issuer}$ med värden ifyllda så är det helt ok.
Tex: PKI kan ser ur så här:



User CA (0): n=77, e=7, d=43, cert=[O:0, I:0, P:77, S:0]
User A (1): n=35, e=7, d=7, cert=[O:1, I:0, P:35, S: 35^43 mod 77 (=63)]
User B (2): n=21, e=7, d=7, cert=[O:2, I:1, P:21, S: 21^7 mod 35(=21)]
User C (3): n=15, e=7, d=7, cert=[O:3, I:2, P:15, S: 15^7 mod 21=(15)]
NOT1: För user 2 och 3 ser vi ett fenomen i RSA som kallas fixpunkter, dvs ett m så att m^d mod n = m.

b) Ja, eftersom CA i en PKI enbart kontrollerar om den publika nyckeln är unik i sin egen PKI domän.

c) Eftersom de meddelanden som utväxlas inte kan spåras från vem de kommer.

d) Med PKI får man nycklar som kan användas för signera meddelanden i DH protokollet och då kan man med hjälp av PKI kontrollera vem som har skickat meddelandet eftersom i certifikatet kopplad till sändaren så har CA i PKI skrivit till vem han/hon har utfärdat certifikatet, dvs vem som signerar.

LYCKA TILL!