Norges teknisk-naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen:
Kristian Gjøsteen 73 59 35 22

EKSAMEN I TMA4155 KRYPTOGRAFI INTRODUKSJON

Bokmål
Torsdag 4. desember 2003
Kl. 9–14

Hjelpemidler (kode D): Enkel kalkulator (HP30S), med tilhørende bruksanvisning
Ingen trykte eller håndskrevne hjelpemidler tillatt.

Sensurdato: 5. januar 2004

Oppgave 1

Forklar hva et blokkchiffer er og hvordan man krypterer med blokkchiffer i ECB-modus (Electronic Code Book) og i CBC-modus (Cipher Block Chaining).

Forklar kort hva som er hovedproblemet med ECB-modus.

En aktiv angriper kan forandre chifferteksten før den når frem til mottageren. Forklar hvordan en aktiv angriper mot CBC-modus kan forandre første blokk av dekrypteringen vilkårlig (han kan invertere fritt valgte bits). Foreslå en måte å stanse slike angrep på.

Oppgave 2

a) Forklar hva en kryptografisk hashfunksjon er.

La $\mathcal{E}(b;k)$ være krypteringsfunksjonen til et blokkchiffer, der b er blokken, k er nøkkelen, og begge er l bit lange. Vi kan bruke $\mathcal{E}$ til å lage en hashfunksjon H på følgende måte: Del meldingen m opp i blokker $b_1, b_2, \ldots, b_r$ (siste blokk polstres med nuller). Sett $s_0 = 0^l$ (l nuller) og bruk regelen $s_i = \mathcal{E}(b_i; s_{i-1})$ til å regne ut $s_1, s_2, \ldots, s_r$. $H(m)$ er da s_r.

Er dette en kryptografisk hashfunksjon?

b) ElGamal-signaturer for korte meldinger lages slik: Den offentlige nøkkelen er (p, g, y), den private nøkkelen er a og meldingen m er et tall $0 < m < p - 1$.

1. Velg k tilfeldig fra $\{1, \ldots, p-2\}$ slik at $gcd(k, p-1) = 1$.

2. Sett r til å være resten av g^k delt på p.

3. Sett s til å være resten av $k^{-1}(m - ar)$ delt på $p-1$, der k^{-1} er en multiplikativ invers til k modulo $p-1$.

Signaturen er (m, r, s), og den verifiseres ved å sjekke at $y^r r^s \equiv g^m \pmod{p}$.

Vis at signaturene produsert av signeringsalgoritmen alltid blir verifisert.

La u, v være tilfeldige, og sett r til å være resten av $y^v g^u$ delt på p, og s er resten av $-rv^{-1}$ delt på $p-1$. Vis at hvis m er resten av su delt på $p-1$, da verifiseres signaturen (m, r, s).

Forklar hvordan man kan bruke kryptografiske hashfunksjoner til å stanse dette angrepet.

Oppgave 3

a) Vis at 2 er en primitiv enhetsrot modulo 59.

b) En offentlig nøkkel for ElGamal er (59, 2, 35).

Krypter meldingen $m = 11$ med denne offentlige nøkkelen. Velg 6 som det tilfeldige tallet.

Du får vite at den private nøkkelen er 24. Dekrypter chifferteksten (55, 23).

c) Du har en annen offentlig ElGamal-nøkkel (59, 2, 36) og en chiffertekst (27, 50). På en eller annen måte har du fått vite at dekrypteringen av (54, 31) er 33. Bruk dette til å finne dekrypteringen av (27, 50).

Hint: $54 \equiv 2.27 \pmod{59}$.

Oppgave 4

a) Forklar hvordan man lager nøkler i RSA. Gi et eksempel der $300 < n < 400$.

b) Et firma vil spare tid på RSA-nøkkelgenereringen og ønsker derfor å bruke samme modulus til alle sine ansatte. For å hindre at ansatte kan lese meldinger sendt til andre ansatte, får alle forskjellige (e, d)-par, slik at to offentlige nøkler har samme modulus, men forskjellig e.

Er dette et godt system? Begrunn svaret.

Oppgave 5

La p være et primtall og la $E : y^2 \equiv x^3 + ax + b \pmod{p}$ være en elliptisk kurve. Beskriv en effektiv algoritme som tar inn kurven E, et punkt $P = (x_1, y_1)$ på kurven og et heltall k, og gir ut punktet kP. Du kan bruke addisjonsoperasjonen på kurven som en subrutine.

Regn ut $5P$ og $10P$ når kurven er $E : y^2 \equiv x^3 + 3x + 7 \pmod{11}$ og $P = (8, 9)$. Kan du utifra dette si noe om hvor mange punkter det er på kurven?

Hint: Følgende formler kan være nyttige:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \lambda = \frac{3x_1^2 + a}{2y_1}, \quad x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1.$$