Norges teknisk–
naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen:
Kristian Gjøsteen 73 59 46 16/73 59 35 20

EKSAMEN I TMA4155 KRYPTOGRAFI, INTRODUKSJON

Bokmål
Torsdag, 8. desember 2005
Kl. 0900-1300

Tillatte hjelpemidler:
godkjent kalkulator

Oppgave 1

I denne oppgaven skal vi arbeide med det engelske alfabetet med de 26 bokstavene A, B, C, ..., Z.

a) Anta at du har en pseudo-tilfeldig tallgenerator som tar som inndata en hemmelig nøkkel, en initialiseringsvektor og et tall n, og gir ut en følge av tall $z_1, z_2, \ldots, z_n$, $0 \leq z_i < 26$. Forklar hvordan du kan bruke denne til å lage et kryptosystem som tar meldinger bestående av bokstavene A, B, C, ..., Z.

b) Alice og Bob kommunisere med et slikt kryptosystem. Du vet at de første 14 tegnene i chifferteksten utgjør initialiseringsvektoren. Alice har sendt de to følgende chiffertekstene til Bob:

BGTGTTFZFHGVRY CXXEHQTBEAWAWX
BGTGTTFZFHGVRY HTJBFAEHBIDWIOH

Finn meldingene. Kan du avgjøre hvilken melding som tilhører hvilken chiffertekst?

Hint: Den første eller den andre meldingen kan inneholde strengen AES.

c) Hvis initialiseringsvektorer velges som tilfeldige bokstavstrenger med lengde 14, gi et grovt estimat for hvor mange chiffertekster man må sende før det er sannsynlig at initialiseringsvektorer blir gjenbrukt.

Oppgave 2

I denne oppgaven er $p = 47$ og $q = 23$.

a) Hva betyr *orden modulo p*?

Vis at $g = 2$ har orden q modulo p.

Formlene for DSA-signering er:

$$r = (g^k \bmod p) \bmod q, \qquad s = k^{-1}(m + ar) \bmod q.$$

Formlene for DSA-verifisering er:

$$u = s^{-1}m \bmod q, \qquad v = s^{-1}r \bmod q, \qquad r \stackrel{?}{=} (g^u x^v \bmod p) \bmod q.$$

b) Bestem hvilke (hvis noen) av de følgende er gyldige DSA melding-signatur-par for den offentlige nøkkelen $(47, 23, 2, 7)$:

$$(13, (13, 14)) \qquad\qquad (12, (13, 14))$$

c) Finn den diskrete logaritmen til 7 til base 2 modulo 47 ved hjelp av Shanks Baby-step-Giant-step-algoritme.

d) Bruk den diskrete logaritmen du fant til å signere meldingen $m = 11$. (Velg $k = 9$.)

Oppgave 3

a) La $p = 19$ og $q = 23$. Velg en passende e og fullfør RSA-nøkkelgenereringen.

b) Forklar hvordan RSA-signatursystemet (uten hashfunksjon) virker, og forklar hvordan du kan konstruere et gyldig melding-signatur-par for den offentlige nøkkelen $(1000216006039, 5)$.

c) Se på den offentlige nøkkelen $(7859101, 5)$. Du får den gyldige signaturen 6717425 for meldingen 555. Finn en gyldig signatur for meldingen 835472.

Hint: Hva er $555 \cdot 835472$ modulo 7859101?