Norges teknisk-naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen:
Kristian Gjøsteen 73 59 35 22

EKSAMEN I TMA4155 KRYPTOGRAFI INTRODUKSJON

Bokmål
Tirsdag 14. desember 2004
Kl. 9–13

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

Sensurdato: 11. januar 2005

Oppgave 1

Dekrypter følgende chiffertekst og forklar hvilket kryperingssystem som er brukt:

QAPPJ YNQ RJI WJXYJS FÆ JPXFRJS

Hint: Klarteksten inneholder ett av de tre ordene DER, FRA eller MED.

Oppgave 2

a) La $p = 47$. Finn et tall g som har orden 23 modulo p. Begrunn svaret.

b) Beskriv Diffie-Hellmans nøkkelutvekslingsprotokoll. Gi et eksempel der Alice og Bob utfører denne protokollen. Bruk p og g fra forrige deloppgave og trekk de tilfeldige tallene fra mengden $\{7, 11, 13, 27\}$.

c) Forklar hva et mann-i mellom-angrep er og hvordan et slikt angrep utføres mot Diffie-Hellmann-protokollen.

Oppgave 3

a) Bruk Pollards $p-1$ - metode til å faktorisere $n = 493$. Vis regningen.

b) Den offentlige nøkkelen i RSA er (n, e) og den private nøkkelen er (n, d). Forklar hvordan n, e og d henger sammen.

Gitt $n = 493$ og $e = 3$, finn d.

c) Forklar kort hva digitale signaturer er og hvordan man kan bruke RSA til å lage slike. Bruk tallene fra forrige deloppgave til å RSA-signere meldingen $m = 2$.

Oppgave 4

La x mod y betegne resten av x delt på y.

I DSA (Digital Signature Standard) er den offentlige nøkkelen $pk = (p, q, g, y)$ og den private nøkkelen $sk = (p, q, g, a)$.

For å signere m velger man k tilfeldig og setter $r = (g^k \bmod q$ og $s = (k^{-1}(m + ar)) \bmod q$.

Signaturen (m, r, s) vertifiseres ved å sette $u_1 = (s^{-1}m) \bmod q, u_2 = (s^{-1}r) \bmod q$ og sjekke at $r = ((g^{u_1}y^{u_2}) \bmod p) \bmod q$.

a) Vis at verifiseringen alltid vil godta signaturer som er generert med signaturalgoritmen.

b) Gitt den offentlige nøkkelen $(10007, 5003, 49, 2580)$ og signaturene $(17, 3152, 4401)$ og $(18, 3152, 662)$, finn det hemmelige tallet a.

Oppgave 5

a) Forklar hva en MAC-algorime er og hva det vil si at den er sikker.

b) I denne oppgaven ser vi bare på meldinger som kan deles opp i et helt antall blokker av lengde n. La $m = m_1||m_2||\cdots||m_l,\ m_i \epsilon \{0,1\}^n$.

En populær konstruksjon for hashfunksjoner er å iterere en kompresjonsfunksjon. Hvis $h' : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$ er kompresjonsfunksjonen beregner man $h(m)$ ved hjelp av iterasjonsreglene $s_{i+1} = h'(s_i, m_i), h(m) = s_{l+1}$ og s_0 er satt til en kjent konstant.

Vi kan lage en MAC-algoritme ved hjelp av h' på følgende måte. MAC (k, m), der k er en hemmelig nøkkel, beregnes ved hjelp av iterasjonsreglene $s_0 = k, s_{i+1} = h'(s_i, m_i)$ og MAC $(k, m) = s_{l+1}$.

Vis at denne MAC-algoritmen er usikker.