Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen:
Kristian Gjøsteen 73 55 02 42/73 59 35 20

EKSAMEN I TMA4155 KRYPTOGRAFI, INTRODUKSJON

Bokmål
Lørdag 2. desember 2006
Tid: 0900-1300
Tillatte hjelpemidler: godkjent kalkulator

Oppgave 1 I denne oppgaven skal vi bruke den offentlige RSA-nøkkelen $(589, 403)$.

a) Gitt at $589 = 19 \cdot 31$, finn den tilhørende private RSA-nøkkelen.

b) Forklar det enkleste RSA-signatursystemet. Beregn en signatur for meldingen $m = 2$. Grei kort ut om noen av sikkerhetsproblemene med dette enkle systemet.

Oppgave 2

a) Bruk Kinesisk restteorem til å finne en løsning på følgende system:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

b) Bruk Pohlig-Hellman-algoritmen til å beregne den diskrete logaritmen av 11 til base 3 modulo 31.

c) Faktoriser 253 med Pollards $p - 1$-metode.

Oppgave 3

a) Forklar hvordan Diffie og Hellman sin nøkkelutvekslingsprotokoll virker, samt hva dens formål og viktigste egenskaper er. Gi et eksempel med $p = 17$ og $g = 2$.

b) Hva er et mann-i-midten-angrep på Diffie-Hellman? Gi et eksempel med $p = 17$, $g = 2$. Skisser et mottiltak mot dette angrepet.

Oppgave 4

a) Forklar hva en hashfunksjon er, og hva preimage-, andre preimage- og kollisjonsmotstandsdyktighet betyr i denne sammenhengen.

Vi ønsker å bruke en kompresjonsfunksjon $f : \{0,1\}^{18} \to \{0,1\}^9$ som en del av en hashfunksjon. Kompresjonsfunksjonen består av tre Feistel-aktige runder på formen

$$L_i||R_i \longmapsto L_{i+1}||R_{i+1} = R_i||(F(R_i) \oplus L_i),$$

og $f(L_0||R_0) = R_3$. Funksjonen $F : \{0,1\}^9 \to \{0,1\}^9$ er definert ved

$$F(x_0, x_1, \ldots, x_8) = S_0(x_0, x_1, x_2)||S_1(x_3, x_4, x_5)||S_2(x_6, x_7, x_8),$$

der S_i er substitusjonsbokser definert ved følgende tabell:

	000	001	010	011	100	101	110	111
S_0	001	010	011	100	101	110	111	000
S_1	111	000	001	010	011	100	101	110
S_2	011	001	000	100	010	111	100	010

b) Regn ut $f(000\,111\,000\,101\,010\,111)$.

c) Finn en kollisjon i f.