Norges teknisk-naturvitenskapelige
universitet
Institutt for matematiske fag

Faglig kontakt under eksamen: Aslak Bakke Buan
Telefon: 5 02 89

Kryptografi, introduksjon, SIF5024

Bokmål
Onsdag 18. desember 2002
Kl. 9–14
Hjelpemidler: Typegodkjent kalkulator
Sensur: 15. januar 2003

Alle svar skal begrunnes.

Oppgave 1 Nummerer bokstavene som følger: A - 0, B - 1, ... , Å - 28. Vi krypterer ved at bokstav nummer x erstattes med bokstav nummer $3x + 5 \pmod{29}$.

a) Finn en dekrypteringsfunksjon på formen $ay + b \pmod{29}$.

b) Dekrypter teksten *BLC VC, BPFØL DHJ*, som er kryptert ved hjelp av denne algoritmen.

Oppgave 2 La $n = 17 \cdot 23 = 391$. La ϕ være Eulers ϕ-funksjon, og $\gcd(a, b)$ være største felles divisor til heltallene a og b.

a) Finn $\phi(n)$.

b) Vis at $\gcd(3, \phi(n)) = 1$, og beregn $d = 3^{-1} \pmod{\phi(n)}$.

c) La $(n, e) = (391, 3)$ være din offentlige nøkkel i et RSA-kryptosystem. Du har mottatt den krypterte meldingen $c = 2$. Hva er klarteksten m?

d) Tre RSA-brukere A, B og C har offentlige nøkler $(n_A, 3)$, $(n_B, 3)$ og $(n_C, 3)$, der $\gcd(n_A, n_B) = \gcd(n_A, n_C) = \gcd(n_B, n_C) = 1$. En melding t krypteres med hver av de tre sin offentlige nøkkel, og gir kryptotekstene c_1, c_2 og c_3. Hvis du kjenner disse tre kryptotekstene og de offentlige nøklene, hvordan kan du finne t?

Oppgave 3

a) Hva er pseudoprimtall?

b) Vis ved hjelp av Fermats test at 341 ikke er et primtall.

c) Forklar Fermats faktoriseringsalgoritme, og illustrer ved å faktorisere 68269.

Oppgave 4

Vi skal se på en variant av ElGamals signatur-algoritme. Nøklene genereres på følgende måte. A velger en stort primtall p og en primitiv rot α for $\mathbb{Z}_p^*$. Hun velger a slik at $0 < a < p-1$ og $\gcd(a, p-1) = 1$, og beregner $\beta = \alpha^a \pmod{p}$. Paret (α, β) er den offentlige nøkkelen, mens a er den private nøkkelen. La $x \in \mathbb{Z}_p$ være meldingen som skal signeres. Signaturen er da paret (γ, δ), der

$$\gamma = \alpha^k \pmod{p}$$

og

$$\delta = (x - k\gamma)a^{-1} \pmod{p-1},$$

der det velges en ny tilfeldig verdi av $k \in \mathbb{Z}_p$ for hver signering.

a) Hvilken fordel har denne algoritmen i forhold til den vanlige ElGamal signatur-algoritmen, med hensyn til effektivitet?

b) Finn en verifiseringsalgoritme.

Oppgave 5 Gitt primtall p og q, og la $n = p \cdot q$. Anta at n og $\phi(n)$ er kjent. Hvordan kan man lett (og effektivt) finne p og q?

Hint: $p + q = n - \phi(n) + 1$.

Hvorfor er dette relevant for sikkerheten i RSA?