Tik-79.159 Tiedon salaus ja suojaus
Tentin 19.11.1996 ratkaisut — Tuomas Aura

1. (a) Hybridisalauksessa itse sanoma salataan symmetrisellä salausmenetelmällä ja satunnaisella istuntoavaimella. Istuntoavain salataan vastaanottajan julkisella avaimella ja lähetetään vastaanottajalle erikseen tai sanoman mukana.

   (b) Heikoilla avaimilla salatut sanomat ovat helpommin avattavissa kuin muilla avaimilla salatut. Pahimmassa tapauksessa salakielinen teksti on sama kuin selväkielinen. Hyvässä salausalgoritmissa heikkoja avaimia on vähän tai ei lainkaan.

   (c) *Brute-force* -hyökkäyksessä käydään kaikki mahdolliset avainvaihtoehdot (tai tekstit tai muut parametrit) läpi ratkaisun löytämiseksi.

   (d) Salauksessa konfuusion tehtävä on häivyttää havaittavat yhteydet selväkielisen ja salakielisen tekstin välillä ja estää selväkielisen sanoman redundanssin havaitseminen salakielisessä. Lohkosalauksessa konfuusio saadaan useimmiten aikaan substituutiolla. (1p)

   (e) Diffuusion tehtävänä on levittää kunkin selväkielisen bitin vaikutus laajalle alueelle salakieliseen tekstiin. Lohkosalauksessa diffuusio saadaan aikaan permutoimalla bittejä. (1p)

   (f) Message Authentication Code MAC on symmetriseen menetelmään perustuva allekirjoitus. Sanoma allekirjoitetaan ja sen alkuperä tarkistetaaan saman salaisen avaimen avulla. MAC-algoritmi voidaan konstruoida esim. yksisuuntaisesta hajautusfunktiosta.

2. (a) $N = 29 \cdot 41 = 1189$. $\varphi(N) = (29-1)\cdot(41-1) = 1120$. Julkinen avain on $e = 17$. Salainen avain d saadaan kaavasta $ed \equiv 1 \pmod{\varphi(N)}$ eli $17 \cdot d + 1120 \cdot k = 1$ Eulerin algoritmilla.

$$
\begin{aligned}
1120 &= 65 \cdot 17 + 15 & \qquad 15 &= 1120 - 65 \cdot 17 \\
17 &= 1 \cdot 15 + 2 & 2 &= 17 - 1 \cdot 15 \\
15 &= 7 \cdot 2 + 1 & 1 &= 15 - 7 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
11 &= 15 - 7 \cdot 2 \\
&= 15 - 7 \cdot (17 - 15) = -7 \cdot 17 + 8 \cdot 15 \\
&= -7 \cdot 17 + 8 \cdot (1120 - 65 \cdot 17) = 8 \cdot 1120 - 527 \cdot 17
\end{aligned}
$$

   $k = 8$ ja $d \equiv -527 \equiv 593 \pmod{1120}$. Salainen avain on siis $d = \mathbf{593}$.

   (b) $M = 321$. $d = 593 = 1001010001_2$.

1	$321^{2^0} \bmod 1089$		$= \mathbf{321}$
0	$321^{2^1} \bmod 1189$	$= 321^2 \bmod 1189$	$= 787$
0	$321^{2^2} \bmod 1189$	$= 787^2 \bmod 1189$	$= 1089$
0	$321^{2^3} \bmod 1189$	$= 1089^2 \bmod 1189$	$= 488$
1	$321^{2^4} \bmod 1189$	$= 488^2 \bmod 1189$	$= \mathbf{344}$
0	$321^{2^5} \bmod 1189$	$= 344^2 \bmod 1189$	$= 625$
1	$321^{2^6} \bmod 1189$	$= 625^2 \bmod 1189$	$= \mathbf{633}$
0	$321^{2^7} \bmod 1189$	$= 633^2 \bmod 1189$	$= 1185$
0	$321^{2^8} \bmod 1189$	$= 1185^2 \bmod 1189$	$= 16$
1	$321^{2^9} \bmod 1189$	$= 16^2 \bmod 1189$	$= \mathbf{256}$

$$
\begin{aligned}
S = M^d \bmod N = 321^{593} \bmod 1189 &= 321^{2^9} \cdot 321^{2^6} \cdot 321^{2^4} \cdot 321^{2^0} \bmod 1189 \\
&= 256 \cdot 633 \cdot 344 \cdot 321 \bmod 1189 = 344 \cdot 344 \cdot 321 \bmod 1189 = 625 \cdot 321 \bmod 1189 \\
&= \mathbf{873}.
\end{aligned}
$$

Allekirjoitus on siis $S = 873$ ja allekirjoitettu sanoma kokonaisuudessaan "Moi, mitä kuuluu?",873.

Arvostelu: Tässä piti osata suurten lukujen potenssiin korotus. Täydet pisteet sai väärästä avaimesta tai pienistä laskuvirheistä huolimatta, jos idea oli oikein. Huomaa, että $321^{17} \neq 321^{593}$ vaikka $321^{17 \cdot 593} = 321$ eli ei kannata yrittää olla liian ovela.

(c) Jukinen avain d (17) vai olla hyvinkin lyhyt, esim. juuri 17. Enintään se voi olla moduulin suuruinen. Moduulin N (1189) pitää olla vähintään 512 bittiä, mielellään enemmän. Hajautusfunktion arvo (321) on luultavasti 128 tai 160 bittinen.

3. (a) B tarkistaa ensin aikaleiman T_A tuoreuden. Hän myös säilyttää vastaanottamansa nonssit N_A niitä vastaavan aikaleiman voimassaoloajan, eikä siksi hyväksy samaa sanomaa kahta kertaa aikaleiman voimassaoloaikanakaan.

   (b) Erityisesti tätä protokollaa koskeva oletus: voidakseen uskoa istuntoavaimen K_{AB} tuoreuteen B joutuu olettamaan, että A todella generoi tuoreen istuntoavaimen. A voisi halutessaan myös kopioida jonkin vanhan tietämänsä istuntoavaimen tai kopioida salatun istuntoavaimen $E_B(K_{AB})$ jostain aiemmasta B:lle tarkoitetusta sanomasta. Toisin sanoen B joutuu luottamaan A:han tässä asiassa.

   Muita oletuksia: A:n julkinen avain hyvä, kellot suurin piirtein samassa ajassa.

   (c) Jos sanomassa ei olisi allekirjoituksen sisällä vastaanottajan tunnusta B, voisi joku nauhoittaan tämän sanoman ja lähettää sen muille vastaanottajille, esim. C:lle. C luulisi A:n haluavan aloittaa kommunikaation hänen kanssaan avaimella $D_C(E_B(K_{AB}))$, joka tietenkin on pelkkää roskaa ja jonka oikeasti vain C tietää.

4. Lagrange-kynnysrakenne on laskettu tuntemattomasta polynomista $y \equiv ax+M \pmod{37813}$. Polynomilta tunnetaan pisteet $(2, 19525)$ ja $(4, 1582)$. Saadaan yhtälöt

$$
\begin{aligned}
a \cdot 2 + M &\equiv 19535 \\
a \cdot 4 + M &\equiv 1582.
\end{aligned}
$$

Ratkaistaan M:

$$
\begin{aligned}
(4a + M) - 2(2a + M) &\equiv 1582 - 2 \cdot 19535 \\
-M &\equiv -37488 \\
M &\equiv 37488.
\end{aligned}
$$

Salainen sanoma on siis 37488. ($a \equiv 28837$.)

Arvostelu: Laskun olivat osanneet lähes kaikki sitä yrittäneet.

5. Diffie–Hellman-avaintenvaihdosta voi kertoa toimintaperiaatteen lisäksi monenlaisia asioita, joita löytyy oppikirjasta, luennoilta ja laskuharjoituksista sekä kirjallisuudesta.

   Arvostelu: Tarkoituksesta ja toimintaperiaatteesta sai 2 pistettä. Diskreetti logaritmi ja *man-in-the-middle* toivat 2 lisää. Mistä tahansa muista tarkennuksista, huomioista tai laajennuksista sai myös pisteitä. Diffie-Hellmanin tulosta ei muuten käytetä suoraan salausavaimena, vaan se on ns. avainmateriaalia, josta avain voidaan tuottaa esim. yksisuuntaisella hajautusfunktiolla.

6. Nollatietotodistuksista verifioija varmistuu siitä, että todistajalla on tiedossaan jokin salaisuus S, mutta salaisuus ei paljastu verifioijalle. Verifioija ei myöskään voi jälkikäteen todistaa kenellekään muulle, että salaisuus S on verifioijan hallussa. (2p)

   Propabilistisissa todistuksissa todistaja esittää verifioijalle kaksi osatehtävää, joiden ratkaisut yhdessä paljastaisivat salaisuuden S. Verifioija valitsee kumman tehtävän ratkaisun hän haluaa nähdä. Tämän jälkeen todistaja esittää pyydetyn ratkaisun. Hän pystyy huijaamaan vain todennäköisyydellä 1/2. Proseduria toistetaan halutun monta kertaa, kunnes verifioija uskoo todistajan tuntevan salaisuuden S. Ulkopuolinen ei vakuutu todistuksesta, koska todistaja ja verifioija ovat voineet sopia valinnoista etukäteen. Verifioija ei myöskään voi välittää todistusta eteenpäin, koska asia tulee todistetuksi vain sille, joka tekee valinnat osatehtävien välillä. (2p) Esim. graafien isomorfismi. (Ovellinen käytävä on oikeastaan huono esimerkki, koska saman asian voi todistaa menemällä toisesta haarasta sisään ja tulemalla toisesta ulos; vaivaa säästyy.) (2p)

   Julkisen avaimen nollatietotodistuksessa todistaja ja verifioija yhdessä generoivat tehtävän, jonka ratkaisun todistaja voi tuntea vain jos hän tuntee salaisuuden S, mutta jonka ratkaisun esittäminen ei kuitenkaan paljasta salaisuutta S. Esim. Guillou-Quisquater. (2p)

   Useimmat nollatietotodistukset ovat interaktiivisia, eikä interaktiivista todistusta voi esittää paperilla. Siksi esimerkin antaminen paperilla on vaikeaa. On kuitenkin olemassa myös ei-interaktiivisia (propabilistisia) todistuksia, jotka voisi periaatteessa esittää paperilla. Niissä verifioijan valinnat tekee jono pseudosatunnaisia bittejä, joilta vaaditaan kaksi ominaisuutta: (1) todistaja ei saa pystyä vaikuttamaan bittien arvoihin merkittävässä määrin. (2) Bittien pitää riippua todistajan asettamista tehtävistä niin, ettei todistaja voi tehtäväpareja valitessaan vielä tietää bittien arvoja. (2p, tätä tarkoitettiin tehtävän toisessa osassa, muttei vaadittu arvostelussa.)

   Nollatietotodistuksia voidaan käyttää esimerkiksi myytävän tiedon aitouden osoittamiseen ennen sen paljastamista. Toinen sovellus on tietokoneiden keskinäiseen tunnistaminen (esim. automaatti ja pankkikortti) ilman, että tunnistaja voi käyttää tietoa myöhemmin hyväkseen. Kalleutensa vuoksi nollatietotodistukset eivät ole lyöneet itseään läpi sovelluksissa, vaan halpa haaste-vastemenettely tai julkisen avaimen allekirjoitus ajaa yleensä saman asian. (2p)

   Vaarana todistuksissa ovat *man-in-the-middle* -hyökkäykset, joissa verifioija välittää valintoja ja vastauksia verifioijan ja kolmannen osapuolen välillä. Näin kolmas osapuoli voi vakuuttua todistettavasta asiasta. Todistaja voi myös olla joukko, joka tekee valintansa niin, että kaikki joukon jäsenet voivat olla varmoja valinnan satunaisuudesta. Näin iso joukko tulee vakuuttuneeksi todistuksesta. (2p)

   Muutakin voisi kertoa. Schneier on innostunut todistusten käytön sosiaalisista vaaroista. (n p)