Tik-79.159 Tiedon salaus ja suojaus	
Tentin 2.9.1997 ratkaisut	Tuomas Aura

1. (a) Salauksessaa diffuusion tehtävänä on levittää kunkin selväkielisen bitin vaikutus laajalle alueelle salakieliseen tekstiin. Lohkosalauksessa diffuusio saadaan aikaan permutoimalla lohkon bittejä ja käyttämällä mahdollisimman suuria S-bokseja.

   (b) Karakteristinen differenssi tarkoittaa salausalgoritmin iteraation (*round*) tiettyä (yleensä erittäin heikkoa) tilastolista ominaisuutta: jos kahdella salattavalla lohkolla on ennen iteraatiota tietty erotus (XOR), voidaan siitä päätellä niiden erotus (XOR) iteraation jälkeen jollakin pienellä, mutta satunaista arvausta paremmalla todennäköisyydellä. Tätä käytetään hyväksi differensiaalisessa kryptoanalyysissa.

   (c) Hajautusfunktion törmäyksettömyys tarkoittaa, että on vaikeaa (käytännössä mahdotonta) löyttää kahta sanomaa, joilla olisi sama sormenjälki.

   (d) OFB-moodissa lohkosalausalgoritmia käytetään bittivirtasalauksen avainvirran tuottamiseen. Salattava sanoma ei vaikuta avainvirtaan. Avainvirta XOR:ataan salattavan sanoman kanssa. $S_0 = IV; S_i = E_K(S_{i-1}, C_i = P_i \oplus S_i$, kun $i = 1, 2, \ldots$ (Kuvakin kelpaisi.)

   (e) Kerkhoffsin periaatteen mukaan salauksen vahvuuden ei pidä riipua algoritmin salaisuudesta. Vain avain on salainen.

   (f) Eksplisiittisessä autentikoinnissa tunnistaja vakuuttuu, että tunnistettava on osallistunut kommunikaatioon autentikoinnin aikana. (Implisiittisessä varmuus toisen läsnäolosta saadaan vasta, kun istuntoavainta käytetään.)

2. (a) Salaus ei yleensäkään suojaa sanomien eheyttä, ainoastaan luottamuksellisuutta. CBC-moodissa voidaan selväkieliseen lohkoon aiheuttaa haluttuja muutoksia kääntämällä bittejä tätä lohkoa edeltävän lohkon salakielestä. (Edellinen lohko tosin muuttuu satunnaiseksi roskaksi, mutta se ei aina haittaa. Ei ainakaan, jos kyseessä on 1. lohko, jolloin edellinen lohko on IV.)

   (b) Satunnaisuutta lisätään ainakin kahdestä syystä: sama sanoma salattuna useaan kertaan näyttää erilaiselta ja kryptoanalyysi vaikeutuu. Lohkosalauksessa satunnaisuutta voidaan lisätä satunnaisella alustusvektorilla (IV) tai satunnaisella täytteellä selväkielisen tekstin seassa. RSA:ssa salattava teksti on usein paljon lyhyempi kuin RSA-lohko (esim. 128-bittien istuntoavain ja 1023-bittinen salattava lohko). Tällöin salattavan tekstin eteen ja jälkeen lisätään satunnaista täytettä.

   (c) Yksityisen avaimen tunteminen mahdollistaisi modulin tekijöiden selvittämisen ja siten toisen yksityisten avainten murtamisen. Jos kaikki avaimet kuuluvat samalle henkilölle, tämä ei haittaa. Tällöinkin saman sanoman salaaminen kahdella eri avaimella, joissa on sama moduli, mahdollistaa sanoman (ei yksityisen avaimen!) selvittämisen (ks. Schneier s. 472).

3. (a) Protokolla jatkuu oman yksityisen eksponentin valitsemisella. Olkoon tämä satunnaisesti väliltä 2–1947 valittu lukuarvo tällä kertaa $y = 117$. Lasketaan oma julkinen avain $Y = g^y \bmod n$.

   $117 = 1110101_2$.

1	$7^1 \bmod 1949$		$= \mathbf{7}$
0	$7^2 \bmod 1949$	$= 7^2 \bmod 1949$	$= 49$
1	$7^4 \bmod 1949$	$= 49^2 \bmod 1949$	$= \mathbf{452}$
0	$7^8 \bmod 1949$	$= 452^2 \bmod 1949$	$= 1608$
1	$7^{16} \bmod 1949$	$= 1608^2 \bmod 1949$	$= \mathbf{1290}$
1	$7^{32} \bmod 1949$	$= 1290^2 \bmod 1949$	$= \mathbf{1603}$
1	$7^{64} \bmod 1949$	$= 1603^2 \bmod 1949$	$= \mathbf{827}$

   $7 \cdot 452 \cdot 1290 \cdot 1603 \cdot 827 \bmod 1949 = 1109$ (kerrotaan vaiheittain redusoiden välillä).

   Julkinen avain $Y = 1109$ lähetetään **allekirjoitettuna** A:lle.

   (b) Lasketaan salainen avainmateriaali $X^y \bmod n$.

1	$1172^1 \bmod 1949$		$= \mathbf{1172}$
0	$1172^2 \bmod 1949$	$= 1172^2 \bmod 1949$	$= 1488$
1	$1172^4 \bmod 1949$	$= 1488^2 \bmod 1949$	$= \mathbf{80}$
0	$1172^8 \bmod 1949$	$= 80^2 \bmod 1949$	$= 553$
1	$1172^{16} \bmod 1949$	$= 553^2 \bmod 1949$	$= \mathbf{1765}$
1	$1172^{32} \bmod 1949$	$= 1765^2 \bmod 1949$	$= \mathbf{723}$
1	$1172^{64} \bmod 1949$	$= 723^2 \bmod 1949$	$= \mathbf{397}$

   $1172 \cdot 80 \cdot 1765 \cdot 723 \cdot 397 \bmod 1949 = 1565$ (kerrotaan vaiheittain redusoiden välillä).

   Salaiseksi avainmateriaaliksi tulee siis 1565.

4. (a) Varjot ovat pistepareja tuntemattomalla polynomilla $y(x) = Ax^2 + Bx + M$. (Tuntemattomia kertoimia on kolme, kun salaisuuden ratkaisuun tarvitaan 3 varjoa. Siksi asteluku on 2.) Pitää ratkaista vakiotermi M. Kirjoitetaan ongelma yhtälöryhmäksi:

$$
\begin{aligned}
A + B + M &= 1123 \\
9A + 3B + M &= 9322 \\
16A + 4B + M &= 16678
\end{aligned}
$$

   Ratkaisu voi tapahtua monella tavalla. Esim. vähennetään 1. yhtälö 2. yhtälöstä ja saadaan $8A + 2B = 8199$. Kertomalla tämä 2:lla ja vähentämällä 3. yhtälöstä saadaan $M = 280$. Niinpä salainen sanoma on 280.

   (b) Ratkaistaan vielä kertoimet A ja B. Välivaiheet voidaan laskea negatiivisilla ja murtoluvuilla, kunhan lopulliset tulokset redusoidaan modulo $2^{16} + 1$. Saadaan $A = 1085.5$ ja $B = -242.5$. Koska (3,7) -kynnysrakenteessa lienee jo varjot x:n arvoilla $1, \ldots, 7$, lasketaan uusi varjo kohdasta $x = 8$. $y(8) = 1085.5 \cdot 8^2 - 242.5 \cdot 8 +$

$280 = 2275$. Tulos on onneksi kokonaisluku, sillä muuten joudut-taisiin laskemaan jakolasku modulokunnassa. Uusi varjo on nyt $(8, 2275)$.

5. (a) Salausfunktion E pitää tässä normaalien symmetriseltä salaukselta vaadittavien ominaisuuksien lisäksi suojata sanoman eheys. Se täytyy siis toteuttaa esim. salaus + MAC -yhdistelmänä. (Valitettavasti vanhoissa protokollakuvauksissa käytetään usein tällaista merkintää.)

   (b) Mallory voi aikaleimoista huolimatta pitää protokollan ja istuntoavaimen K_{SES} elossa mielivaltaisen pitkään. Myöhemmin hän saattaa saada istuntoavaimen tietoonsa ja esiintyä A:lle B:nä tai B:lle A:na.

$$
\begin{array}{ll}
A \to T: & A, E_A(T_A, B, K_{SES}) \\
T \to B: & E_B(T_T, A, K_{SES}) \\
M(B) \to T: & B, E_B(T_T, A, K_{SES}) \\
T \to M(A): & E_A(T_{T2}, B, K_{SES}) \\
M(A) \to T: & A, E_A(T_{T2}, B, K_{SES}) \\
T \to M(B): & E_B(T_{T3}, A, K_{SES}) \\
M(B) \to T: & B, E_B(T_{T4}, A, K_{SES}) \\
T \to M(A): & E_B(T_{T5}, B, K_{SES}) \\
\ldots & \\
M \to T: & A, E_B(T_{T1234}, A, K_{SES}) \\
T \to B: & E_B(T_{T1234}, A, K_{SES})
\end{array}
$$

   (c) Syynä hyökkäykseen on, että sanomat 1 ja 2 ovat saman näköisiä. Tämä voidaan korjata lisäämällä sanomiin tyyppikenttä:

1.	$A \to T:$	$A, E_A($"WMF message 1"$, T_A, B, K_{SES})$
2.	$T \to B:$	$E_B($"WMF message 2"$, T_T, A, K_{SES})$

   Muitakin mahdollisia korjauksia on.

   (d) Eksplisiittinen tyypitys.

   (e) B tunnistaa A:n eksplisiittisesti eli tietää protokollan lopussa A:n halunneen yhteyttä häneen. A tunnistaa B:n implisiittisesti, koska ei saa tältä yhtään sanomaa protokollan aikana. A varmistuu vasta istuntoavaimella suojatun kommunikoinnin alettua, että B on läsnä.

6. Anonyymistä sähköisestä rahasta voi kertoa toimintaperiaatteen lisäksi monenlaisia asioita, joita löytyy oppikirjasta, luennoilta ja laskuharjoituksista sekä kirjallisuudesta.

   Täysiin pisteisiin riittäisi ainakin Ecashin toiminnan tarkka kuvaus tai sähkörahan tavoitteiden ja toimintaperiaatteiden laaja yleisempi selostaminen.