T-79.159 Tiedon salaus ja suojaus
2005 / Tentti
16.5.2005

1. (6 pist) Kun japanilainen hävittäjäalus upotti amerikkalaisen partioveneen PT-109, jonka päällikkönä oli luutnantti J. F. Kennedy, australialainen radioasema otti vastaan seuraavan Playfair menetelmällä salatun viestin:

   `KX JE YU RE BE ZW EH EW RY TU HE YF SK RE HE GO YF`

   `IW TT TU OL KS YC AJ PO BO TE IZ ON TX BY BW TG ON`

   `EY CU ZW RG DS ON SX BO UY WR HE BA AH YU SE DQ`

   Tulkitse ensimmäinen rivi. Käytetty avain oli *royal new zealand navy*. Joitakin siirtovirheitä on voinut esiintyä.

   Jos et muista miten Playfair toimii voit yrittää saada kolme lohdutuspistettä (3 pist) tulkitsemalla seuraavan viestin:

   ```
   M  E  T  J
   A  E  Y  N
   X  H  O  E
   ```

2. (a) (2 pist) Mitä on kolminkertainen salaus ja mitä etua siitä on?

   (b) (2 pist) Miksi 3DES salausoperaation keskimmäinen operaatio on tulkintaoperaatio ennemminkin kuin salausoperaatio?

   (c) (2 pist) Mitä on hybridisalaus?

3. Olkoon $p = 17$, $q = 13$ ja $e = 7$ RSA parametreja.

   (a) (3 pist) Määritä salainen avain $d$.

   (b) (3 pist) Tulkitse salakieliteksti $C = 128$.

4. Tarkastellaan polynomiaritmetiikkaa käyttäen polynomia $x^3 + x + 1$ kolmebittisten kokonaislukujen joukossa.

   (a) (3 pist) Määritä luvun $6 =$ `110` diskreetti logaritmi kantaluvun $2 =$ `010` suhteen.

   (b) (3 pist) Määritä luvun $3 =$ `011` käänteisluku.

5. Counter Mode PRNG tunnetaan mys nimellä Cyclic Encryption PRNG.

   (a) (2 pist) Esitä kuinka Counter Mode PRNG toimii käyttäen IDEA salausalgoritmia. Minkäkokoista laskuria käyttäisit?

   (b) (2 pist) Kun tunnetaan yksi tai useampi Counter Mode PRNG algoritmin tuottama bittilohko, voidaanko sanoa jotain saman PRNG:n tuottamista muista lohkoista tuntematta salaista avainta?

   (c) (2pist) Mihin tällaista PRNG algoritmia voidaan käyttää käytännän turvallisuusjärjestelmissä?