Övning i kryptografi

Daniel Bosk*

25 juni 2011

1. **Konstruera en krypteringsapparat.** Den ska kunna användas för att kryptera och avkryptera ett meddelande. Krypteringsalgoritmen är valfri, det får vara en känd metod (Caesarchiffer, substitutionschiffer eller Vigenèrechiffer), en variant av dessa eller ett helt eget chiffer.

2. **Kryptera ett meddelande.** Kryptera ett meddelande till en kompis utan att berätta innehållet och låt kompisen kryptera ett hemligt meddelande till dig. Försök att knäcka varandras kryptering.

3. **Knäck chiffret.** Du jobbar som kryptoanalytiker åt Försvarets Radioanstalt (FRA) och får följande text på ditt skrivbord.[1]

   ```
   VJGOCFJCVVGTUVGCRCTVUWPFGTYC
   KVKUKPVJGWUWCNRNCEGDGJKPFVJGEWTVCKP
   ```

   Vad betyder det?

*Kontakt: dbosk@kth.se.

[1] Om du har tillgång till dator är http://www.simonsingh.net en bra sida för fördjupning och verktyg. På http://en.wikipedia.org/wiki/Letter_frequency finns tabeller och diagram över bokstavsfrekvenser.