Kapitulli 1

Hyrje në kriptografi

Detyra për ushtrime

1. Dekriptoni tekstin e shfruar

   EHJLQWKHDWWDFNQRZ

   të enkriptuar me shifruesin e Caesar-it. Sa është vlera e çelësit të përdorur?

   Udhëzim: Shih Java klasën `Exc0101`

2. Dekriptoni tekstin e shifruar

   OVDTHUFWVZZPISLRLFZHYLAOLYL

   të enkriptuar me një shifrues me zhvendosje. Sa është vlera e çelësit të përdorur?

   Udhëzim: Shih Java klasën `Exc0102`

3. Dekriptoni tekstin e shifruar

   JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZ
   QQOCIBZKLFAFGQVFZFWWEOGWOPFGFHWOLPHLRLOL
   FDMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJV
   FPFWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLRO
   QVFGWJVFPFOLFHGQVQVFILEOGQILHQFQGIQVVOSF
   AFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOC
   GFHX

   të enkriptuar me shifruesin me zëvendësim mono-alphabetic. Shfrytëzoni histogramin nga figura 1.1.

   Udhëzim: Shih Java klasën `Exc0103`

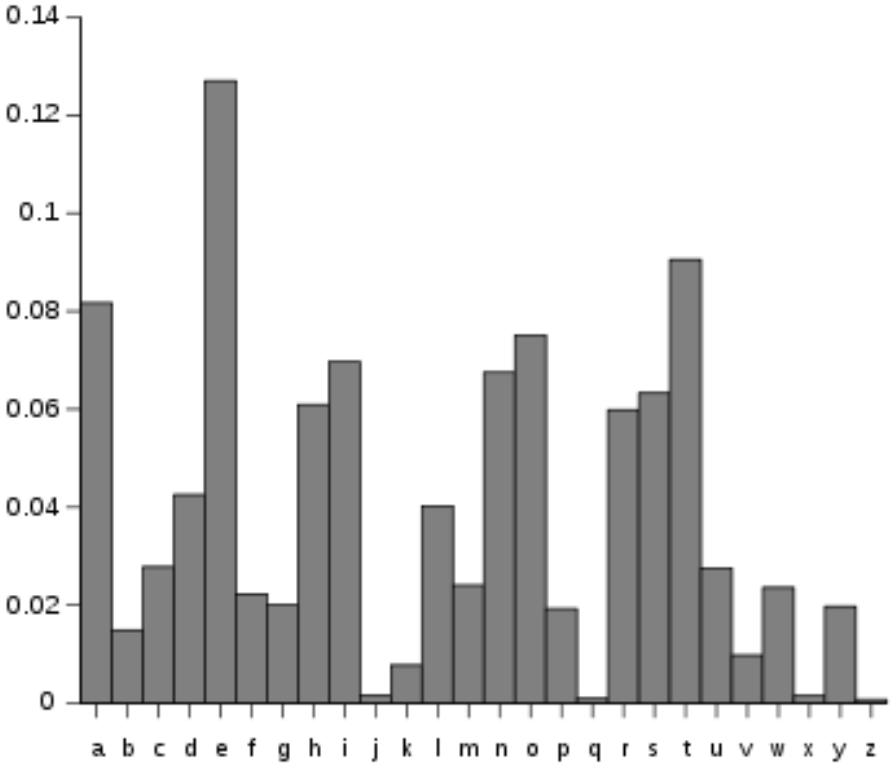

Figura 1.1: Frekuenca relative e shkronjave për tekst në gjuhën angleze

4. Supozoni se dëshironi të enkriptoni një mesazh të vetën $M \in \{0,1,2\}$ dukë përdorur një çelës të rastësishëm të përbashkët $K \xleftarrow{\$} \{0,1,2\}$. Supozoni se e bëni këtë duke paraqitur K dhe M me anë të dy bitëve $\{00,01,10\}$ dhe pastaj duke vepruar me XOR në paraqitjet: $C = K \oplus M$. A është ky një protokol i sigurtë? Shpjegoni.

5. Supozoni se dëshironi të enkriptoni një mesazh të vetën $M \in \{0,1,2\}$ dukë përdorur një çelës 2-bitësh të rastësishëm të përbashkët. Shpjegoni një mënyrë të mirë për të bërë këtë.

6. *Enkriptim simetrik me një shpil kartash.* Alice përzien një shpil kartash dhe ia shpërndan të tërin vehtes dhe Bob-it (secili prej tyre merr në mënyrë të rastësishme nga 26 karta). Alice tani dëshiron t'ia dërgojë një mesazh sekret M Bob-it duke thënë diçka me zë. Përgjuesja Eve është duke dëgjuar: ajo dëgjon çdo gjë që thotë Alice (por Eve nuk mund t'i shohë kartat).

   (a) Supozoni se mesazhi i Alice është një string 48 bitësh. Shpjegoni se

si Alice mund t'ia komunikojë M Bob-it në atë mënyrë që Eve të mos ketë asnjë informatë se ç'është M.

(b) Tani supozoni se mesazhi i Alice është 49 bit. Vërtetoni se nuk ekziston protokol i cili i lejon Alice t'i komunikojë M Bob-it në atë mënyrë që Eve të mos ketë informatë mbi M.

Udhëzim: Shih Maxima skriptin `cryptography-exc-01.wxm`

7. Jepni përkufizimin formal të skemave kriptografike për:

   (a) shifruesin me zhvendosje;

   (b) shifruesin me zëvendësim monoalfabetik.

8. Shifruesi polialfabetik (Vigener) funksionon duke aplikuar shifrues të shumfishtë zhvendosjeje në varg. Kështu, zgjedhet një fjalë e shkurtër sekrete si çelës, dhe pastaj mesazhi tekstual enkriptohet duke „mbledhur" secilin karakter të tekstit me karakterin vijues të çelësit (sikur në shifruesin me zhvendosje), duke përsëritur çelësin ku është e nevojshme. Për shembull, një enkriptim i mesazhit

   tell him about me

   duke përdorur çelësin

   cafe

   do të funksiononte si në vijim:

Mesazhi:	`tellhimaboutme`
Çelësi:	`cafecafecafeca`
Kodi:	`WFRQKJSFEPAYPF`

   Jepni përkufizimin formal të skemës kriptografike për shifruesin polialfabetik.

9. *Sulmi i mesazhit të njohur (known-plaintext attack).* Në këtë skenar kundërshtari mëson një ose më tepër çifte mesazh/tekst-i-shifruar të enkriptuar nën të njëjtin çelës. Qëllimi i kundërshtarit është që pastaj të përcaktojë mesazhin e enkriptuar në ndonjë tjetër tekst të shifruar. Tregoni se

   (a) shifruesi me zhvendosje;

   (b) shifruesi me zëvendësim monoalfabetik;

   (c) shifruesi me zëvendësim polialfabetik (shih detyrën 8)

   është trivial për t'u thyer duke përdorur një sulm të mesazhit të njohur. Sa tekst mesazhi është e nevojshme të dihet për ta kthyer të tërin çelësin për secilin shifrues?

10. *Sulmi i mesazhit të zgjedhur (chosen-plaintext attack).* Në këtë sulm kundërshtari ka aftësinë të marrë enkriptimet e mesazheve sipas dëshirës. Pastaj, përpiqet të përcaktojë mesazhin që është enkriptuar në ndonjë tjetër tekst të shifruar. Tregoni se

    (a) shifruesi me zhvendosje;

    (b) shifruesi me zëvendësim monoalfabetik;

    (c) shifruesi me zëvendësim polialfabetik (shih detyrën 8)

    është trivial për t'u thyer duke përdorur një sulm të mesazhit të zgjedhur. Sa tekst mesazhi është e nevojshme të dihet që kundërshtari ta kthejë të tërë çelësin? Krahasoni me detyrën paraprake.