Kodutöö

1. Uuri laviini efekti erinevates algoritmides kasutades internetis olevaid standardseid lahendusi. Kursuse lehel asub DES lahendus javas <http://www.tlu.ee/~matsak/crypto/JceSunDesTest.java> , kus teiste algoritmide jaoks saab teha vajalikud muudatused. Blowfish algoritmi jaoks saad koodi siit: <http://www.tlu.ee/~matsak/crypto/blowfish_java.rar> . Abiks on samuti java spetsifikatsioon <http://docs.oracle.com/javase/8/docs/api/javax/crypto/package-summary.html>, vaata näiteks klassi nimega [Cipher](http://docs.oracle.com/javase/8/docs/api/javax/crypto/Cipher.html).

Laviini efekti on uuritud ka teadlaste poolt, vaata näiteks <http://www.ijettcs.org/Volume1Issue3/IJETTCS-2012-10-25-097.pdf>

Siin olev ülesanne aitab aru saada, et kuidas rakendada ühte krüptoanalüütikas tuntud meetodit algoritmide turvalisuse taseme testimiseks.

Täida allolev tabel:

|  |  |  |
| --- | --- | --- |
| Krüpterimisvõti nr 1 tekstina ja kahendkoodis |  |  |
| Krüpterimisvõti nr 2 tekstina ja kahendkoodis |  |  |
|  | Krüpteerimise tulemus DES algoritmiga kahendkoodis | Krüpteerimise tulemus kolmekordse DES algoritmiga kahendkoodis | Krüpteerimise tulemus Blowfish algoritmiga kahendkoodis | Krüpteerimise tulemus AES algoritmiga kahendkoodis |
| Sinu nimi kahendkoodis: |  |  |  |  |
|  | 1 |  |  |  |
| 2 |  |  |  |
| Nimi kahendkoodis ühe vahetatud bitiga (märgi punaseks) |  |  |  |
|  | 1 |  |  |  |
| 2 |  |  |  |
| Muudetud bittede % krüptogrammis võrreldes esialgse krüpteerimisega | 1 |  |  |  |
| 2 |  |  |  |

1. Seletada (kirjalikult) samm-sammult algoritmi RC6 põhimõtteid oma nime/perekonnanime kaheksa esimese järjest paikneva tähe šifreerimise näitel.
2. Uuri algoritm Twofish. Tee seda samm sammult.

Olgu võtmeks Sinu nimi koos perekonnanimega.

Pikenda võtit kuni standardse pikkuseni 128.

Esita Baitide massiivina m0...m15.

Samuti M massiivina.

Arvuta alamvõti K0.

Näita ühe raundi krüpteerimist lähtudes sellest, et K8 ja K9 on suvalised vajaliku pikkusega alamvõtmed (mõtle ise välja) ja sisendtekstiks on sinu matriklinumbrist moodustatud tekst.

1. Leia internetis vahendeid juhuslike arvude genereerimiseks. Vali nendest kaks ja esitada nende analüüs seletades genereerimise põhimõtet ja esitades tõenäosusliku jaotust graafiliselt (näiteks joondiagrammi abil).