Informazio Sistemen Segurtasuna Kudeatzeko Sistemak 2023/2024

1 laborategia – Zifraketa

Helburuak:

1. Zifraketa eta informazio ezkutaketa oinarrizko teknikak erabiltzen ikastea.
2. Oinarrizko kriptoanalisi teknikak ikastea.
3. Laburpen algoritmoekin lan egin.

Baliabideak:

- Ubuntu (Erabiltzailea/pasahitza: lsi/lsi).
- Egela-ko “1 Laborategia - Zifraketa” karpeta.

1.- Maiztasun analisiaren bidezko kriptoanalisia

Hurrengo mezua desenkriptatzen gai den programa sortu (Jatorrizko mezua gazteleraz idatzia dago):

RIJ AZKKZHC PIKCE XT ACKCUXJHX SZX, E NZ PEJXKE, PXGIK XFDKXNEQE RIPI RIPQEHCK ET OENRCNPI AXNAX ZJ RKCHXKCI AX CJAXDXJAXJRCE AX RTENX, E ACOXKXJRCE AXT RITEQIKERCIJCNPI OKXJHXDIDZTCNHE AX TE ACKXRRCIJ EJEKSZCNHE.

AZKKZHC OZX ZJ OERHIK AX DKCPXK IKAXJ XJ XT DEDXT AX TE RTENX IQKXKE XJ REHETZJVE XJ GZTCI AX 1936. DXKI AZKKZHC, RIPI IRZKKX RIJ TEN DXKNIJETCAEAXN XJ TE MCNHIKCE, JI REVI AXT RCXTI. DXKNIJCOCREQE TE HKEACRCIJ KXvITZRCIJEKCE AX TE RTENX IQKXKE. NZ XJIKPX DIDZTEKCAEA XJHKX TE RTENX HKEQEGEAIKE, KXOTXGEAE XJ XT XJHCXKKI PZTHCHZACJEKCI XJ QEKRXTIJE XT 22 AX JIvCXPQKX AX 1936, PZXNHKE XNE CAXJHCOCRERCIJ. NZ PZXKHX OZX NCJ AZAE ZJ UITDX IQGXHCvI ET DKIRXNI KXvITZRCIJEKCI XJ PEKRME. NCJ AZKKZHC SZXAI PEN TCQKX XT REPCJI DEKE SZX XT XNHETCJCNPI, RIJ TE RIPDTCRCAEA AXT UIQCXKJI AXT OKXJHX DIDZTEK V AX TE ACKXRRCIJ EJEKSZCNHE, HXKPCJEKE XJ PEVI AX 1937 TE HEKXE AX TCSZCAEK TE KXvITZRCIJ, AXNPIKETCLEJAI E TE RTENX IQKXKE V OERCTCHEJAI RIJ XTTI XT DINHXKCIK HKCZJOI OKEJSZCNHE.

OHARRA: “Zifraketa simetrikoa” gaiko 20-22 gardenkiak.

2.- Esteganografia eta laburpen algoritmoak

Buenaventura Durruti-k mezu garrantzitsu bat idatzi du zuentzako, **irudia.zip** karpetako irudi batean. Esaldia StegoSuite (Ubuntu) programaren bidez sartu da, pasahitz barik. Mezua daukan irudiak hurrengo Hash (MD5) kodea du:**e5ed313192776744b9b93b1320b5e268**. Zein artxibo da? Zer dio esaldiak?

Norbaitentzako mezu sekretu bat irudi batean sartu nahi baduzu, eta hartzailearen aurrean ez dagoela aldaketarik egon bermatu, zelan egingo zenuke?

Informazio Sistemen Segurtasuna Kudeatzeko Sistemak 2023/2024

Artxibo baten edukian bere laburpen kriptografikoa sartzea posiblea al da? Hau da, fitxategi honen laburpen kriptografikoa eduki moduan kopiatu ahal da barnean, konprobazioa egiteko?