SEMINAR IZ KRIPTOGRAFIJE

DES

Robert Petek

FMF

2. marec 1998

Na zadnjem seminarju smo:

- klasična kriptografija
- razbijanje klasičnih tajnopisov
- rešitev domače naloge o Siru Johnu
- rešitev domače naloge iz Preseka
- domače naloge iz prvega poglavja
- R. Petek: simetrična kriptografija in DES

Današnji načrt

- R. Petek: DES (nadaljevanje) (do str. 88)
- iščemo dobrovoljca za
  diferencialno kripto-analizo
- reševanje nalog 1. in 3. poglavja

Obvestilo:

Informacije o učbeniku: Cryptography, Theory and Practice, najdete na domači strani, vključno z 'errata list'.

Namesto, da si kupite učbenik, bi si morda lahko naročili CD-ROM.

Essential Books on Cryptography and Security from Dr. Dobb's Journal.

CD vsebuje 12 odlično napisanih knjig iz kriptografije in stane US$99.95. Dr. Dobb's Journal domača stan pravi, da bodo začeli CD-je pošiljati februarja.

Žal pa na njihovi domači strani piše tudi naslednje:

Due to U.S. Government Restrictions, this CD-ROM is only available for customers in the U.S. and Canada.

Domača naloga za študente
Bojana Moharja:

1) 1.2

2) 3.2

Bonus: Vigenerjev tajnopis
(vsak posebej ga dobi od mene po pošti)

Do naslednjega tedna

- končajte z branjem 3.poglavja (str. 113)

- končajte z reševanjem nalog iz
3. poglavja (str. 110-113)

Stinsonovega učbenika
Cryptography, Theory and Practice

Prihodnjič:

- A. Habič končala s 3. poglavjem (diferencialna kripto-analiza)

- morda bo M. Masnoglav začel s 4. poglavjem (RSA)