

Tentamen Cryptografie

30 maart 2006

Bachelor/Master op het tentamenpapier te vermelden!

1. [10 punten] - Inleiding

Laat zien hoe twee correspondenten met behulp van *quantum cryptografie* een bit-rij kunnen uitwisselen.

2. [10 punten] - Klassieke systemen

Ontvangen is het volgende Eerste Wereldoorlog-bericht:

CHI-134

GGXAF AGXFD ADFAF AXEXA XDAXA XGAFA XXFXF GDFAG XXDAX
AGFDF XDFFA XDXFF DAAFA ADAXD AGDXA AAGGA DGGFA FAFDD
AFAGD XAFDX GAGDP GGXFD XFDDX DFAGF AXGAA ADAFA ADFF

- De substitutiesleutel luidt KAISERWILHELM.
Geef het hierop gebaseerde 5x5-sleutelvierkant ($I=J$).
- De transpositiesleutel luidt VATERLANDSLIEBE.
Geef de bijbehorende numerieke sleutel.
- Ontcijfer het bericht met de gegeven sleutels.

3. [10 punten] - Klassieke systemen

- Leg uit hoe een cryptografische rotor werkt.
- Beschrijf de constructie van de Duitse Enigma.

4. [10 punten] - Statistische methoden

- Het tweede moment $\sum_i p_i^2$ van een symbooldistributie speelt in de cryptoanalyse een belangrijke rol. Geef een voorbeeld van een toepassing.
- Geef de formule voor de zuivere schatter waarmee dit tweede moment uit een frequentietelling wordt berekend.
- Waarvoor wordt bij twee distributies f^1 en f^2 de Chi-test $\chi = \sum_i f_i^1 f_i^2$ gebruikt?

5. [10 punten] - Moderne systemen

- Hoe werkt TripleDES?
- Waarom niet DoubleDES?
- Wat is het effect van het sleutelschema $K_1 = K_2 = K_3$?

6. [10 punten] - Public Key

- Beschrijf het ElGamal-systeem. *Bachelors behoeven de details van de vercijfering niet te geven, van masters worden die wel verlangd.*
- Waarin verschilt ElGamal van RSA?

7. [10 punten] - Informatietheorie

- Gegeven is een symbooldistributie p_A, p_B, \dots, p_Z voor de 26 letters van het alfabet. Geef de formule voor de entropie van deze distributie.
- Wat zijn de minimale en maximale waarden van deze entropie en bij welke distributies worden deze aangenomen?
- Leg beknopt uit wat in de cryptografie wordt bedoeld met het begrip *unicity distance*.

8. [10 punten] - Schuifregisters

- Een bepaalde combinatie van drie schuifregisters S_1, S_2 en S_3 heeft de nevenstaande productietabel. Bepaal de terugkoppelfunctie in algebraïsche normaalvorm.
- *Voor bachelors:*
Beschrijf de Siegenthaler correlatie-aanval.
- *Voor masters:*
Beschrijf (in grote lijnen) de Meier-Staffelbach correlatie-aanval.

S_1	S_2	S_3	S
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

9. [10 punten] - Schuifregisters

Geef een beschrijving van de A5/1 algoritme zoals gebruikt in mobiele telefoons (de precieze karakteristieke functies behoeven niet te worden gereproduceerd).