

Opgave 1: Ontvangen is het volgende WW1 cryptogram in het ADFGX-systeem:

10

CHI 134
 GGXAF AGXFD ADFAF AXFXA XDAXA XGAF A XXFX XGDFAG XXDAX
 AGPDF XDFFA XDXFF DAAFA ADAXD AGDXA AAGGA DGGFA FAFDD
 AAFAG XAFDX GAGDD GGXFD XFDDX DFAGF AXGAA ADAFA ADFF

- Maak een 5x5-substitutievierkant met sleutel KAISERWILHELM. Laat de J weg.
- Maak een transpositiesleutel van VATERLANDSLIEBE.
- Ontcijfer met deze sleutels het cryptogram.

Opgave 2:

15

- Wat is een cryptografische rotor en hoe kunnen rotors gebruikt worden? Welke transformatie bewerkstelligt een rotor?
- Geef een zo volledig mogelijke beschrijving van de Duitse Enigma codeermachine.
- Welke instellingsparameters kent de Enigma?
- U bent chef-cryptoanalyst tijdens het Ardennen-offensief van 1944. Een van uw medewerkers vermoedt een boodschap aan generaal Von Rundstedt in handen te hebben en probeert nu de crib VONRUNDSTEDT te passen op de cijfertekst XHGJP NGGDF KM. U vertelt hem zijn tijd daaraan niet te verdoen. Waarom?

Opgave 3:

5

- Welke statistische grootte wordt met de φ -test bepaald?
- Wat kan men voor een cryptogram hiermee constateren?
- Wat wordt met de χ -test bepaald?

Opgave 4: De regel van Bayes toegepast op een systeem met berichten $\{\mathcal{M}\}$, cryptogrammen $\{\mathcal{C}\}$ en sleutels $\{\mathcal{K}\}$ geeft als de voorwaardelijke kans op een bericht M gegeven een bericht C :

10

$$P(M|C) = \frac{P(M)P(C|M)}{P(C)}$$

Beschrijf in woorden wat dit betekent en laat zien onder welke omstandigheden de best mogelijke veiligheid wordt bereikt. Geef ook aan wat dit betekent voor het aantal sleutels in de sleutelverzameling $\{\mathcal{K}\}$.

LET OP! Deze opgave is uitsluitend voor studenten in een master-opleiding. Zij slaan de volgende opgave over, want die is alleen voor bachelor-studenten.

Opgave 5:

10

- Gegeven is een symbooldistributie $p_A, p_B \dots p_Z$ voor de 26 letters van het alfabet. Geef de formule voor de entropie H van deze distributie.
- Wat is de laagst mogelijke waarde en bij welke distributie is dat het geval?
- Wat is de hoogst mogelijke waarde en bij welke distributie is dat het geval?
- Definieer hetgeen onder de *unicity distance* wordt verstaan.
- De unicity distance kan worden benaderd met de formule $\frac{H(K)}{H_0 - H_\infty}$. Wat is de betekenis hierin van de grootheden $H(K)$, H_0 en H_∞ ?
- Wat zegt de unicity distance van een cryptosysteem wel en wat zegt deze niet over de cryptanalyse ervan?

Opgave 6: Geef een zo uitvoerig mogelijke beschrijving van het Feistel-schema voor een geheimschrift.

10

Hoe werkt het vercijferen en ontcijferen in dit schema? Wat zijn de eigenschappen van deze methode?

Opgave 7: Welk effect hebben de zwakke en halfzwakke sleutels in DES en waardoor ontstaat dat effect?

5

Opgave 8: Beantwoord de volgende vragen over het RSA-systeem.

- Wat zijn de parameters van het systeem?
- Welke van de parameters zijn openbaar en welke geheim?
- Hoe worden de parameters gekozen?
- Hoe gaan het verscijferen en ontcijferen in z'n werk?
- Hoe groot is de bloklengte?
- Waarop berust de veiligheid van het systeem?

15

Opgave 9:

- Een bepaalde combinatie van drie schuifregisters $S1$, $S2$ en $S3$ heeft de nevenstaande productietabel. Bepaal de terugkoppelfunctie in algebraïsche normaalvorm.
- Tegen welk van de deelregisters kan met success een correlatieaanval worden ondernomen en waarom?

$S1$	$S2$	$S3$	S
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

10

Opgave 10:

- Teken het verbindingsschema van de terugkoppelfunctie behorend bij een lineair schuifregister met als karakteristieke functie:

$$f(x) = 1 + x^2 + x^3 + x^4 + x^8$$

- Aan welke eis moet een terugkoppelfunctie voldoen om een maximaalrij te genereren?
- Hoe groot is de periode van een maximaalrij? Verklaar ook kort waarom.
- Verklaar waarom een maximaalrij voldoet aan het eerste criterium van Golomb voor een goede random bitrij.

10