

Opgave 7:

10

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

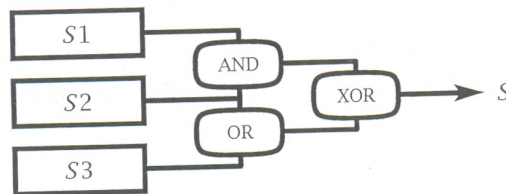
$$f(x) = 1 + x^2 + x^3 + x^4 + x^8$$

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

Opgave 8:

10

- a. Werk de productietabel uit voor de sleutelstroom van de in de figuur gegeven combinatie van drie schuifregisters.



- b. Bepaal de terugkoppelfunctie behorend bij deze sleutelstroom in algebraïsche normaalvorm.
 c. Bereken de correlatie tussen de uitvoerstream en elk van de drie samenstellende schuifregisters.

Opgave 9:

10

bestemd voor bachelor studenten

Geef een beknopte uitleg van de Siegenthaler correlatie-aanval op een schuifregistercombinatie.

bestemd voor master studenten

Geef een beknopte uitleg van de Meier-Staffelbach correlatie-aanval op een schuifregistercombinatie.

Let op. Beknopt betekent niet onvolledig. Bedoeld is dat mag worden afgezien van uitvoerige exercities met formules, maar de essentiële feiten moeten wel opgeschreven worden. Beschrijf dus waarop de aanval berust, hoe deze wordt opgezet, wat er moet worden gedaan.

Opgave 1:

Ontcijfer met behulp van sleutel LIBERAAL het volgende cryptogram in de enkelvoudige kolomtranspositie met onuitgevuld transpositieblok:

OEPDG OSMLE EETTT ONDKS TDTFE OTCEE ERSEA ENJME NDZDE IGENL
NTRRF REOHN

5

Opgave 2: Het vercijfersysteem is Vigenère.

a. Vercijfer de volgende klaartekst met sleutel ABCD. Maak zelf het benodigde deel van het Vigenère-tableau aan en toon dit.

BANGE STUDENTEN VREZEN DE DOCENTEN EN LANGE TENTAMENVRAGEN

b. Dezelfde klaartekst is met eveneens berichtsleutel ABCD vercijferd, maar nu staat een gepermuterd cijferalfabet in het Vigenère-tableau; het klaaralfabet blijft het standaard alfabet. Het cryptogram luidt nu:

OOIWN QTXEB IVNHX SNKLJ EBBMR BIVNH LJDOI WNSLJ QOHAG VQELB

Bepaal hieruit voor zover als mogelijk de gebruikte permutatie van het cijferalfabet.

10

Opgave 3:

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

5

Opgave 4:

- 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?

10

Opgave 5:

- Geef een zo gedetailleerd mogelijke beschrijving van AES, de Advance Encryption Standard. **Bachelors** mogen de onderliggende algebraïsche formules achterwege laten, maar van **Masters** wordt verlangd hier iets over te vertellen.
- Waarin verschilt de AES fundamenteel van de DES?
- Waarom is er geen behoefte aan een triple-AES?

15

Opgave 6: 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 vercijferen en ontcijferen in z'n werk?
- Hoe groot is de bloklengte?
- Waarop berust de veiligheid van het systeem?

15