Subject: stream cipher
year:2011/1012
Division: security
Examiner: Enas tariq
Date:24/5/1012
Answer (six) Question Only

Note: 10 mark for all question

Q1/ Answer for Tow only:
   A- Explain the Self-synchronizing stream ciphers in detail.
   B- Irreducible polynomials, primitive Explain with example.
   C- Cipher block chaining Mode.

Q2/ Sequence s of length n =160, check the sequence is random or not (used basic statistical tests). Obtained s by replicating the following sequence four times:

```
11100 01100 01000 10100 11101 11100 10010 01001
```
mark(10)

Q3/ Explain Geffe generator, Hardmard generator (figure and equation).

Q4/ By using the random key from initial state 1001 generator as a secret key, n=3 encryption the word "security".

Q5/ what do you mean by a Galois LFSR with drawing.

Q6/ discuss in details LFSR/FCSR summation/parity cascade with algorithm

Q7/ what is the important element for design a stream cipher?

GOOD LUCK