University of Technology
Computer Science Department
Class: 2th information security Branch
Time: 3 hours

Subject: Stream Cipher
Examiner: *Dr. Alaa k.*

Final Exam / 2010 -2011

Note: ***Answer ALL questions.***

Q1/ Write program in **C++** by using **Class** or **Function** (**choose only Two**):

- **Shrinking** Generator.
- **J-K** Flip Flop Generator.
- Shift register four times to the left. (Register length is **4-bits**)
- **Euler's** function. 10 Marks

Q2/ Choose only **One**

A- Use **Berlekamp-Massey** algorithm to find **L** (**Complexity**)
Let $S^n = 011$ where $n = 3$

B- Use the **Geffe** generator to perform the following :

- **Draw** an electronic circuit.
- **Write** the output equation of the **Geffe** generator.
- **Run** generator to find the output sequence. 10 Marks

Q3/ Answer the following:

A- Encode the word "**Stream**" by using the random key generated from **hardmard** generator.

B- Compute the **Addition** and **Multiplication** operations of the following equation:

$$F(X) = X^3 + X^2 + 2$$

$$G(X) = X^2 - X + 1$$

15 Marks

Q4/ **Explain in detail of the following :** (Choose only **Three**)

A- Self-synchronizing stream ciphers.
B- Irreducible and primitive polynomials with examples.
C-RC4.
D- Cipher Feedback Mode. 15 Marks

Q5/ **Discuss the following systems** (Choose only **Two**)

- Pless's
- Multiplexor
- Adder
- Correlation attacker 10 Marks

Q6/ 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 10 Marks