# Final Exam-First Try 2009-2010

*Computer Science Department (Software, Artificial, System branches )*

*Fourth Class, Data Security*

*Ass. Prof. Dr. Soukaena Hassan Hasheem*

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

**Part one (answer one question only): 10 marks**

Q1: explain in details Cryptographic Random Number Generators.

Q2: explain in details Cryptanalysis and Attacks on Cryptosystems

**Part two (answer one question only): 10 marks**

Q1: write fast exponential procedure with simple example.

Q2: write inverse procedure with simple example.

**Part three (answer three questions questions): 30 marks**

Q1: encrypt and decrypt using Vigenère and Beaufort where (plaintext = IRaqi ) and (key = H4).

Q2: explain in details the Exponential cipher scheme then, using Pohlig-Hellman Scheme to encrypt and decrypt $M = 5$ that if $p = 11$, Choose $d = 7$ and compute $e = inv(7, 10) = 3$.

Q3: explain in details the Exponential cipher scheme then using RSA Scheme to encrypt and decrypt $M = 5$ that if $p = 11$ and $q=3$ , Choose $d = 7$ and compute $e = inv(7, 10) = 3$.

**Q4:** explain in details the two methods of Knapsacks (Merkle-Hellman and Diffe-Hellman) then using Diffe-Hellman to encrypt and decrypt $m$=5 that if S=[1,2,4,9], w=15, w'= 8, n=17.

**Part four (answer one question only): 10 mark**

Q1: explain briefly encryption and decryption in DES, support your explanation with figure.

Q2: explain briefly One Round in DES, support explanation with figure.

**Part five (answer one question only): 10 marks**

Q1: explain the work of LFSR key generator in stream cipher (with full example for encryption and decryption, choose the plaintext, polynomial and initial state as you desire).

Q2: explain the work of Geffe Generator in stream cipher(with full example for encryption and decryption, choose the plaintext, polynomials and initial state as you desire).

***Good Luck***