The purpose of the term paper / project is to acquaint you with some of the current literature in cryptology and data security, give you the opportunity to acquire a thorough understanding in a particular topic area, or allow you the chance to do some original research. The term paper / project is selected from one of the areas discussed in the textbook or some other area of your choice related to cryptology. The term paper / project can consist of:

- a survey of a particular area with a critique of the major papers (3 to 5) in the area
- cryptanalysis of a published cryptography scheme
- experimenting and statistically analyzing a published cryptographic scheme
- original research on a cryptographic problem that you define.

The term paper / project is written in the style of a journal publication, limited to no more than eight (8) pages. You are free to choose either an IEEE publication style or an ACM publication style. Links to information about these styles are found on the course web site.

The term paper / project is due on Monday, May 15, 2017 at 6:00 p.m. – the end of the scheduled time for the final exam. You will also give a 15 minute presentation about your term paper / project with a few minutes for questions after the presentation that will be separately scheduled.

Some recommended journals are:

- *Journal of Cryptology*
- *Cipher*
- *IEEE Transactions on Information Theory*
- *Communications of the ACM*
- *Cryptologia*
- *AFIPS National Computer Conference Proceedings*

Examples of recent student Papers/Projects:

1. Theory of Cryptography
   a. High Performance Joint Secret Advanced LDPC Cryptcoding
   b. An Introduction to Certificateless Public Key Cryptography
   c. Evaluating the SHA-256 and Elliptic Curve Digital Signature Algorithms in Bitcoin Transaction
   d. A Look at IKE: Analysis, Implementation, and Improvements

2. Public Key Cryptography
   a. An Analysis of Public-Key Encryption
   b. A Comprehensive Survey of Public Key Cryptography
3. Elliptic Curves
   a. Elliptic Curve Cryptography (ECC) and Its Simulation Using C++
   b. Elliptic Curve Digital Signature Algorithm in Bitcoin
   c. Choosing Safe Elliptic Curves for Use in Cryptography

4. Discrete Logarithms
   a. Perfect Forward Secrecy and the Choice of Ephemeral Diffie-Hellman in SSL
   b. Breaking Diffie-Hellman and Solving Discrete Logarithms

5. Factoring Composite Numbers
   a. Integer Factorization Methods of Different Paradigms

6. Zero-Knowledge Protocols
   a. Zero-Knowledge Proofs
   b. A Study of Zero Knowledge Proofs
   c. Zero Knowledge Proofs: A Look at the Fiat-Shamir Identification Protocol
   d. Introduction and Application of Zero-Knowledge Protocol
   e. Zero Knowledge Protocols in Modern Cryptography

7. Lightweight Block Codes
   a. Survey of Lightweight Cryptographic Methods
   b. Project Research on Implementation, Efficiency, and Comparison of Simon and Speck Family of Lightweight Block Ciphers
   c. Different Implementations of Cryptographic Techniques for Resource Constrained Devices

8. Nonlinear Feedback Shift Registers
   a. Introduction to Stream Cipher and RC4

9. Authentication Systems
   a. Authentication Systems Overview
   b. A Survey of Authentication Standards FIPS 190 and FIPS 196
   c. Graphical Password Schemes: A Survey
   d. Graphical Passwords
   e. An Analysis of Security Flaws and Privacy Concerns Regarding Biometric Authentication Systems, and a Brief Overview on Suggestions to Alleviate these Concerns

10. Key Distribution
    a. Survey of Key Distribution Methods: An Analysis of Four Key Distribution Methods
    b. Survey and Comparison of Two State Quantum Key Distribution Protocols
    c. Quantum Cryptography: Key distribution-The Hackers’ Nightmare
11. Digital Signature Schemes
   a. Digital Signature Systems
   b. Digital Signatures: The Principle and the Schemes
   c. ElGamal Algorithm Used in Digital Signature
   d. Signature Schemes: RSA Signature Scheme and ElGamal Signature Scheme
   e. Critique of the Signcryption Scheme - With Emphasis on Zheng Research
   f. Evaluating the SHA-256 and Elliptic Curve Digital Signature Algorithms in Bitcoin Transaction
   g. The Signature of Multi-User Settings
   h. Cryptanalysis of Multi-Signature Schemes

12. Network Security
   a. A Comprehensive Survey of Network Security
   b. Network Security Overview
   c. A Comparison of Several Cryptographic Techniques and Protocols to Create Secure Communications for a Variety of Networks
   d. A Survey of TLS Protocol and Implementation Weaknesses and their Impacts
   e. Wireless Network Security
   f. A History and Analysis of 802.11 Security Standards
   g. Message Authentication Code
   h. Perfect Forward Secrecy and the Choice of Ephemeral Diffie-Hellman in SSL
   i. Network Security of Internet of Things
   j. Security Considerations and Vulnerabilities in Cloud Computing Networks

13. Quantum Cryptography
   a. Quantum Cryptography Overview
   b. Survey and Comparison of Two State Quantum Key Distribution Protocols
   c. Quantum Cryptography : Key distribution-The Hackers’ Nightmare

14. Cryptanalysis
   a. Breaking the Enigma
   b. Cryptanalysis of Public Key Cryptography
   c. Cryptanalysis of Various Encryption/Decryption Schemes: SHA-1
   d. The Autopsy of WEP
   e. Breaking Diffie-Hellman and Solving Discrete Logarithms

15. General Applications
   a. Payment Security
   b. Echeloned IJTAG Data Protection
   c. Reversible Watermarking
   d. Comparison of Various Encryption Algorithms for Security of Smart Cards
16. Biometric Applications
   a. Biometrics in Modern Cryptographic System
   c. An Analysis of Security Flaws and Privacy Concerns Regarding Biometric Authentication Systems, and a Brief Overview on Suggestions to Alleviate these Concerns

17. Data Base Applications
   a. Database Security: Survey Study on Defense against SQL Injection Attack