1. **Instructor:**

Dr. Song Fang (songf@ou.edu)
Office hour: T&R 1:30pm to 3:00pm in DEH 232
Class meetings: T&R 3:00pm to 4:15pm in CEC 438

2. **Teaching Assistant:**

Mr. Edwin Yang (helloworld2edwin@ou.edu)
Office hour: TBD, in DEH 210

3. **Course Description**

The course is a study of fundamental concepts and principles of computer security. The course covers basic security topics, including symmetric and public key cryptography, digital signatures, cryptographic hash functions, authentication pitfalls, and network security protocols.

4. **Course Objectives**

By the end of this course, students will understand basic security terms such as plaintext, cipher-text, encryption/decryption, and authentication. Students will be able to explain the basic number theory required for cryptographic applications, and manually encrypt/decrypt and sign/verify signatures using cryptographic approaches. Students will be able to identify typical security pitfalls in authentication protocols, and outline the protocols, i.e., AH and ESP protocols, for IP Security.

5. **Student Learning Outcomes:**

By the end of the course, students will:
1. Be tested on core computer security problems in the tests or quizzes.
2. Implement at least two key security algorithms regarding public key and symmetric key cryptographic operations as part of their assignments.
3. Finish at least four homework assignments.
4. Design, implement, or use security techniques learned in the course as part of their project.

6. **Recommended Textbook:**


7. Tentative Schedule:

(These will be adjusted based on the actual progress in a semester.)

T1. Basic Security Concepts (1 lecture)
   - Confidentiality, integrity, availability
   - Security policies, security mechanisms, assurance

T2. Basic Cryptography (1 lecture)
   - Historical background
   - Transposition/Substitution, Caesar Cipher
   - Introduction to Symmetric crypto primitives, Asymmetric crypto primitives, and Hash functions

T3. Secret Key Cryptography (5 lectures)
   - Data Encryption Standard (DES)
   - Encrypting large messages (ECB, CBC, OFB, CFB, CTR)
   - Multiple Encryption DES (EDE)

T4. Message Digests (3 lectures)
   - Applications
   - Strong and weak collision resistance
   - The Birthday Paradox
   - MD5, SHA-1

T5. Public Key Cryptography (5 lectures)
   - Number theory: Euclidean algorithm, Euler Theorem, Fermat Theorem, Totent functions, multiplicative and additive inverse
   - RSA, Selection of public and private keys

T6. Authentication (4 lectures)
   - Basic concepts of identification and authentication
   - Password authentication
   - Authentication protocols

T7. Trusted Intermediaries (2 lecture)
   - Public Key infrastructures
   - Certification authorities and key distribution centers
   - Kerberos

T8. Real-time Communication Security (5 lectures)
   - IPsec: AH and ESP
   - IKE
8. Grading:

- Assignments 20%, project 20%, midterm 20%, final 30%, quiz 10%
- The final grades are computed according to the following rules:
  - A+: >= 95%
  - A: >= 90% and < 95%
  - A-: >= 85% and < 90%
  - B+: >= 80% and < 85%
  - B: >= 75% and < 80%
  - B-: >= 70% and < 75%
  - C+: >= 65% and < 70%
  - C: >= 60% and < 65%
  - C-: >= 56% and < 60%
  - D: >= 53% and < 56%
  - E: >= 50% and < 53%
  - F: < 50%.

9. Policies on late assignments:

For each day an assignment is late - up to a maximum of 3 days, the grade is reduced 15%. For example, if you submit a 90%-correct assignment 2 days late, your overall assignment score will be 60%.

10. Policies on absences and scheduling makeup work:

There will be no makeups for homework assignments. Make-up exams will not normally be permitted. Exceptions will be made if a student presents a police report or a doctor’s note that shows some emergency situation.

11. Academic integrity:

It is the mission of the University of Oklahoma to create an academic culture that fosters student integrity both in and out of the classroom. A student must complete his/her tests, projects and assignments on his/her own. A student's signature on any tests, projects and assignments indicates that the student neither gave nor received unauthorized aid. Academic misconduct is defined as any act which improperly affects the evaluation of a students academic performance or achievement. It specifically includes cheating, plagiarism, fabrication, fraud, destruction of property, and bribery or intimidation, as well as assisting others or attempting to engage in such acts. It is the responsibility of each student to be familiar with the definitions, policies and procedures concerning academic misconduct. For more information, please see http://integrity.ou.edu

12. Accommodation:

The University of Oklahoma is committed to providing reasonable accommodation for all students with disabilities. Students with disabilities who require accommodations in this course are requested to speak with the instructor as early in the semester as possible.
Students with disabilities must be registered with the Disability Resource Center prior to receiving accommodations in this course. The Disability Resource Center web site is located at [http://www.ou.edu/drc/](http://www.ou.edu/drc/)

*Every part of this syllabus is subject to adjustment as the semester progresses. If you are dissatisfied with the course policies, grading, and assignments, please contact the instructor. Reasonable requests for modifications may be accommodated at the instructor’s discretion.*