Dept Number	**CS 408**	**Course Title**	**Applied Cryptography**
Semester Hours	**3**	**Course Coordinator** SP15	**Bidyut Gupta**
Catalog Description	This course is a comprehensive introduction to modern cryptography, with an emphasis on the application and implementation of various techniques for achieving message confidentiality, integrity, authentication and non-repudiation. Applications to Internet security and electronic commerce will be discussed. All background mathematics will be covered in the course.		

Textbooks

SP15

Cryptography & Network Security, William Stallings, 6th Edition, 2013, ISBN: 9780133354690.

References

- Alfred Menezes, Paul van Oorschot and Scott Vanstone, Handbook of Applied Cryptography, CRC Press, 1997. (Available at: http://www.cacr.math.uwaterloo.ca/hac).
- Bruce Schneider, Applied Cryptography, 2nd Ed., John Wiley & Sons, 1996.
- Douglas Stinson, Cryptography: Theory and Practice, 3rd Ed., CRC Press, 2006.
- William Stallings, Cryptography and Network Security, 4th Ed., Prentice Hall, 2006.
- Charlie Kaufman, Radia Perlman and Mike Speciner, Network Security: Private Communication in a Public World, 2nd Ed., Prentice Hall, 2003.
- Neal Koblitz, a Course in Number Theory and Cryptography, Springer-Verlag, 2nd Ed., 1994.

Course Learning Outcomes

- To understand the design principles of modern cryptographic algorithms.
- To learn a variety of cryptanalytic and side-channel attacks.
- To understand how cryptography is deployed in practice, with an emphasis on its application in network security.
- To learn how to implement cryptographic algorithms with symbolic computation software.

Assessment of the Contribution to Student Outcomes

FA13

Outcome →	1	2	3	4	5	6	7	8	9	10
Assessed →	X	X	X	X	X	X				

Prerequisites by Topic

CS 330 with a grade of C or better and MATH 221.

Major Topics Covered in the Course

1. Symmetric-key encryption: classical ciphers, one-time pad, stream ciphers (RC4), Feistel networks, DES, AES, modes of operation {8 classes}
2. Message integrity: hash functions, Merkle's Meta method, parallel collision search, message authentication codes (CBC-MAC, HMAC) {5 classes}
3. Key escrow and secret sharing {2 classes}
4. Public-key encryption: RSA, ElGamal, padding schemes, semantic security {9 classes}
5. Signature schemes: RSA, DSA, ECDSA {3 classes}
6. Pseudorandom bit generation: random bit generation, cryptographically strong pseudorandom bit generators, Yao’s Theorem {2 classes}
7. Key establishment and management: key distribution centers, Diffie-Hellman and station-to-station key agreement, Merkle authentication trees, certificate authorities, public key infrastructures {3 classes}
8. Deployed cryptography: Kerberos, PGP, SSL/TLS, WEP/WPA, digital payment systems (SET, e-cash, micropayments), electronic voting {6 classes}
9. Selected advanced topics: zero-knowledge proofs, strong password protocols (EKE/STP), identity-based encryption, broadcast encryption, oblivious transfer {2 classes}

Latest Revision: Summer 2015