Course Title: Cryptology and Security

1 Objective of the course

Objective of the course is to impart and teach some basic aspects of cryptography. Cryptography consists of two major parts viz Private Key Cryptography and Public key cryptography. The students are taught all basic cryptographic primitives in both these areas of cryptography. In Private Key Cryptography the following basic primitives are taught to get a feel about what Private Key Cryptography is all about.

- Private Key Encryption Schemes: Standard existing notions of security are taught in this course. To get a feel, the students also learn how to construct a secure private key encryption schemes from pseudo-random functions. Since private key encryption schemes are used heavily in practice, detailed construction of DES and AES - two crypto standards - are taught.
- Cryptanalytic Techniques: Known Plain Text Attack and Cipher Text Only Attack on LFSR based cryptosystem have been discussed to give the students a feel how cryptanalysis is performed. In this direction, Linear and Differential Cryptanalysis have been described in detail.
- Perfect secrecy: The notion of perfect secrecy is introduced and some examples given. Though perfectly secret encryptions are desirable, the students learn why such encryption schemes are not used in practice.
- Hash Functions: The use of hash functions and various notions of security are introduced. The inter-relation between these security notions is taught. As in the case of private key encryption schemes, hash functions are used heavily in practice. Popular hash functions like SHA1 and SHA2 are taught in this course.
- Message Authentication Code(MAC): This is another important primitive that the students learn in this course. They also learn how to construct a secure MAC from a pseudo-random functions. In Public Key Cryptography, the two important public key encryption schemes viz RSA and ElGamal schemes are taught in great details. Here also important security models for public key encryption schemes are taught. The students also learn, as part of attacks on these schemes, various factoring algorithms and algorithms for discrete logarithm.
- Signature: Signature is another important primitive in public key cryptography that the students learn in this course. The RSA signature scheme is introduced and shown to be insecure. The stu-

dents also learn how to obtain a secure RSA signature scheme under some hardness assumption. The Digital Signature Algorithm(DSA) – a NIST standard – is also taught.

- Quantum Cryptography: In post quantum era, quantum cryptography will play an important role. Hence, to prepare the students for post quantum situation, the basics of quantum paradigm has been taught. Algorithms like Deutsch-Jozsa [2], Bernstein-Vazirani [1] and Simon [5] have been discussed. Grover [3] and Shor [4] algorithms have been referred (not discussed in detail) to highlight the huge impact of quantum cryptanalysis.

2 Learning Outcome

The learning outcome of this course is reflected partially from the marks obtained in the examinations and the assignments. The students were able to demonstrate the use of various cryptographic primitives. More interaction with the students is desirable so that they can demonstrate how much of the course they could digest and comprehend. In this extra-ordinary situation, we are forced to organize online classes and examinations. Online interaction is not sufficient to understand the students' learning output completely. However, it seems to be satisfactory.

References

[1] E. Bernstein and U. Vazirani. Quantum complexity theory. Proceedings of the 25th Annual ACM Symposium on Theory of Computing, (ACM Press, New York, 1993), 11–20.

[2] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. Proceedings of Royal Society of London, A439:553–558 (1992).

[3] L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th Annual Symposium on the Theory of Computing (STOC)*, May 1996, pages 212–219. Available at `http://xxx.lanl.gov/abs/quant-ph/9605043`

[4] P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Foundations of Computer Science (FOCS) 1994, page 124–134, IEEE Computer Society Press.

[5] D. R. Simon. On the power of quantum computation. SIAM journal on computing. 1997 Oct; 26(5): 1474-83.

Cryptology and Security

- Syllabus
  1. Introduction to Cryptography
     (a) Elementary number theory
     (b) Pseudo-random bit generation
     (c) Elementary cryptosystems
  2. Basic security services: confidentiality, integrity, availability, non-repudiation, privacy
  3. Symmetric key cryptosystems
     (a) Stream Cipher
     (b) Block Ciphers: DES, IDEA, AES
     (c) Hash Functions
     (d) Authentication
  4. Public Key Cryptosystems
     (a) RSA, ECC
     (b) Digital signatures
  5. Security Applications
     (a) Electronic commerce (anonymous cash, micro-payments)
     (b) Key management
     (c) PGP
     (d) Zero-knowledge protocols, fairness
  6. A brief introduction to Quantum & Post-Quantum Cryptography
- Recommended Texts
  1. D. R. Stinson: Cryptography, Theory and Practice, CRC Press
  2. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone: Handbook of Applied Cryptography, CRC Press
  3. N. Koblitz: A course in number theory and cryptography, GTM, Springer
  4. W. Stallings: Cryptography and Network Security
  5. R. Anderson: Security Engineering, Wiley
  6. M. A. Nielsen and I. L. Chuang: Quantum Computation and Quantum Information, Cambridge University Press