Lecture plan for Applied Cryptography

20 March, 2025

The suggested reading for the lecture topics are updated each week after the lecture. The recommended book *Understanding Cryptography* is abbreviated as UC.

Lecture	**Topic**	**Suggested reading**
1	Intro to cryptography; block cipher; encryption modes	Lecture slides, UC[Ch 5.1], uploaded material/link
2	Message authentication code; Introduction to TLS; MAC in TLS	Lecture slides, uploaded material/link
3	Cryptanalytic attack on Encryption mode; Telegram messaging app; Encryption mode in Telegram	Lecture slides
4	Meet-in-the middle attack; Cryptanalytic attack on 2DES, 3DES	Lecture slides, UC[Ch 5.2, 5.3.1, 5.3.2]
5	Hash functions; SHA1 and SHA2; Time memory trade-off attack	Lecture slides
6	Attack on password hashing; Cryptanalytic attack on MD4, MD5	
7	Public-key cryptography, RSA, Diffie-Hellman, ElGamal	
8	Digital Signature; Forging signature	
9	SSL library for crypto: a gentle introduction	
10	PKI and CA, forging certificates	
11	PRNG, PRNG in practice, breaking PRNGs	
12	Key-derivation function; HKDF and application in Signal	