DCC030/049 : Criptografia -- teoria e aplicações

Prof. Jeroen van de Graaf Departamento de Ciência da Computação — ICEX — UFMG

EMENTA

Com o avanço do computador e das redes de telecomunicação, a questão da segurança se torna cada vez mais complicada. Podemos dividir um sistema de computação em componentes:hardware, sistema operacional, redes, software para banco de dados, software para aplicações inclusive aplicações web, etc.

A criptografia é uma área muito importante neste contexto. Trata-se de técnicas matemáticas proporcionando a comunicação e computação segura e confiável na presença de partes maliciosas. Esta área proporciona propriedades básicas de segurança, como a confidencialidade, a integridade e a não-retratabilidade de dados e transações. Ela possibilita, por exemplo, a comunicação segura através de um canal inseguro. Também realiza protocolos seguros para fazer qualquer tipo de computação distribuída, como dinheiro eletrônico, eleições, ou um leilão na internet. Uma parte significativa do curso será dedicada a estudar seus fundamentos matemáticos, para que o aluno possa apreciar o que a segurança criptográfica realmente quer dizer.

Objetivos

Os objetivos principais desta disciplina são:

- estudar os princípios básicos e as primitivas básicas da criptografia, como os métodos principais de ciframento, assinaturas digitais, integridade e autenticidade de dados e de pessoas, etc.
- em particular, saber distinguir entre segurança incondicional, segurança computacional, e segurança ad-hoc.
- conhecer as boas práticas da criptografia, e saber distinguir mitos de fatos.
- saber como a criptografia é aplicada na prática.

Programa

#	Module title	Module content
0	Introduction and overview	Coin flipping (par ou ímpar), Encryption, Hamiltonian Circuit in ZK; overview course; overview of the field
1	Probability, entropy, complexity	Bayes theorem, interpretation of probabilities, Shannon entropy, mutual information, min-entropy, relevance complexity theory and cryptography
2	History and terminology	Vigenère, OTP, simulated OTP (stream ciphers,

		CTR mode); work factor, types of attacks, (brute force, analytical attacks), types of security, large and small numbers
3	Block ciphers	DES, finite fields, AES, modes, attacks
4	Computational algebra and number theory	Cyclic groups, primes, euler phi, fast exponentiation, proving primality, factoring, breaking DLog
5	Public key crypto	DHKE, ElGamal, attacks; RSA, attacks; elliptic curves, attacks
6	Message integrity and authenticity	CRCs, hash functions, collisions, birthday paradox, MACs, (OAEP); digital signatures (RSA, DSA, ECDSA)
7	Key distribution	Needham-Schroeder, Kerberos; hybrid crypto; certificates, PKI
8	Randomness	PRNG, Block Cipher, Hash, CSPRNG, True randomness, Post Processing
9	User authentication, challenge-and-response	passwords, multi-factor, PAKE, knowing square root, knowing DLog
10	Quantum	quantum cryptography, quantum computation, post-quantum cryptography (McEliece, …)
11	Advanced protocols	coin flipping, bit commitment, boolean circuits, homomorphic encryption, voting, multi-party computation