Introdução à Criptografia

(Doutor Pedro Quaresma, Departamento de Matemática, Universidade de Coimbra)

Objectivos da Unidade Curricular

Apreender as noções de criptografia e criptoanálise. Compreensão, do ponto de vista matemático e computacional, de alguns sistemas de criptografia actuais.

Programa

1. Introdução à criptografia: noções básicas.
2. Noções de teoria dos números relevantes em criptografia.
3. Criptografia clássica: cifras mono-alfabéticas e cifras poli-alfabéticas; cifra de deslocamento simples, cifra de deslocamento linear e cifra de Vigenère
4. Criptoanálise: introdução; definição; tipos de ataques. Criptoanálise das cifras clássicas: análise de frequências; índices de coincidência.
5. Cifras Fieira. Cifra de Vernam.
6. Sistemas de criptografia de chave simétrica.
   (a) Cifras Fiestel.
   (b) Cifra FEAL.
   (c) Cifra Advanced Encryption Standard (AES).
   (d) Criptoanálise das cifras deste tipo.
7. Sistemas de criptografia de chave pública.
   (a) Funções unidirecionais e funções unidirecionais com escapatória.
   (b) Cifras de chave pública. Autenticação e manutenção de chaves públicas.
   (c) RSA: definição; implementação, a biblioteca GMP.
   (d) Criptoanálise da cifra RSA: Questões relacionadas com a segurança do método RSA. Algoritmos de factorização: algoritmo de Fermat, Pollard $p-1$ e curvas elípticas.
   (e) Cifra de chave pública Elgamal: geração das chaves; algoritmos de encriptação e desencriptação.
   (f) Problemas de Teoria dos Números relacionados com a cifra Elgamal: problema de Diffie-Hellman e problema do logaritmo discreto em Z_p^*. Cálculo de logaritmos discretos: algoritmo de Shanks. Cálculo de logaritmos discretos: algoritmo do cálculo de índices e algoritmo de Pohlig-Hellman. Logaritmo discreto num grupo cíclico arbitrário. Cifra de chave pública Elgamal num grupo cíclico arbitrário.

Competências Genéricas

- Capacidade de generalização e abstracção;
- Capacidade de formular e resolver problemas;
- Competência na utilização de ferramentas computacionais;

- Conhecimento de resultados matemáticos;
- Concepção ou utilização de modelos matemáticos para situações reais;
- Capacidade de investigação;
- Imaginação e criatividade;
- Capacidade de trabalho em equipa;
- Capacidade de aprendizagem autónoma;
- Espírito crítico.

Métodos de Ensino

Exposição teórica; Proposta de projectos a resolver com acompanhamento por parte dos professores.

Bibliografia

- Vaudenay, Serge, *A Classical Introduction to Cryptography, Applications for Communications Security*, Springer, 2006.
- Buchmann, J., *Introduction to Cryptography*, Springer, 2000.
- Douglas, S. *Cryptography: Theory and Practice*, Chapman & Hall/CRC, 2006.
- Jones, G.A. e Jones J.M., *Elementary Number Theory*, Springer-Verlag, 1998.
- Meneses, A., van Oorschot, P., Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, 1996.
- Queiró, J.F., *Teoria dos Números*. `http://www.mat.uc.pt/~jfqueiro/TN2008.pdf`.
- Ribenboim, P., *The Little Book of Big Primes*, Springer-Verlag, 1991.
- D. Bressoud, S. Wagon. *A Course in Computational Number Theory.* Key College, Publishing, 2000.