

Algebra per codici e crittografia

Luca Giuzzi

Anno Accademico 2015–16

1 OBIETTIVI

Il fine di questo corso è quello di presentare alcune tecniche di base, a carattere algebrico, fondamentali per la crittografia e la teoria dei codici, nonché esempi concreti del loro effettivo utilizzo.

In particolare, si vogliono fornire nozioni sufficienti per poter comprendere in dettaglio crittosistemi moderni quali AES, RSA e i protocolli basati su curve ellittiche, enucleandone pregi e limitazioni.

Osserviamo che le medesime tecniche, oltre che per problematiche di *network security*, si rivelano particolarmente significative anche per l'implementazione di alcune tipologie di codifica di sorgente (codici correttori a blocchi). Questo secondo filone, tradizionalmente legato alla trasmissione numerica dell'informazione, riveste un crescente interesse nello studio di sistemi *software* per l'immagazzinamento dati in memorie intrinsecamente inaffidabili, quali quelle a stato solido.



2 PROGRAMMA

1. Introduzione alla crittografia; crittografia classica e moderna; protocolli di comunicazione.
2. Modelli di attacco e nozioni di sicurezza. Crittografia a chiave segreta e a chiave pubblica.
3. Richiami di teoria dei gruppi.
4. Algoritmi crittografici basati sul logaritmo discreto: Diffie-Hellman, El-Gamal e varianti.

5. Aritmetica modulare e elementi di teoria dei numeri.
6. Il crittosistema RSA e sue varianti; OAEP.
7. Algoritmo euclideo esteso, polinomi e campi finiti.
8. Da DES ad AES.
9. Elementi di crittoanalisi algebrica.
10. Curve ellittiche: il gruppo dei punti e sue applicazioni alla crittografia.
11. Protocolli basati su bilinear pairing fra gruppi.
12. Schemi per key-escrow ed ID-based encryption.
13. Protocolli a conoscenza zero ed anonimità.
14. Applicazioni al problema dell'e-voting
15. Crittosistemi omomorfici.
16. Codici correttori lineari a blocchi.
17. La costruzione dei codici ciclici; motivazioni e proprietà.
18. Codici di Reed-Solomon e BCH; trasformata discreta di Fourier.
19. Codici LDPC e turbo-codes.
20. Codici di rete.
21. Conclusioni.



3 BIBLIOGRAFIA

▷ TESTI PRINCIPALI

1. W. Stallings, "CRYPTOGRAPHY AND NETWORK SECURITY, Prentice Hall (2010)
2. L. Giuzzi, "CODICI CORRETTORI", Springer-Verlag Unitext 25 (2006).

▷ TESTI CONSIGLIATI

1. M.W. Baldoni, C. Ciliberto, G.M. Piacentini Cattaneo, “ARITMETICA, CRITTOGRAFIA E CODICI”, Springer Verlag Unitext 24 (2006)
2. G.W. Bard, “ALGEBRAIC CRYPTANALYSIS”, Springer-Verlag (2006).
3. C. Cid, S. Murphy, M. Robshaw, “ALGEBRAIC ASPECTS OF THE ADVANCED ENCRYPTION STANDARD”, Springer-Verlag (2006).
4. M.J. Hinek, “CRYPTOANALYSIS OF RSA AND ITS VARIANTS”, Chapman and Hall/CRC (2010).
5. A.Joux, “ALGORITHMIC CRYPTANALYSIS”, Springer-Verlag (2009).
6. N. Koblitz, “A COURSE IN NUMBER THEORY AND CRYPTOGRAPHY”, Springer-Verlag (1994).
7. N. Koblitz, “ALGEBRAIC ASPECTS OF CRYPTOGRAPHY”, Springer-Verlag (1996).
8. R.J. McEliece, “THE THEORY OF INFORMATION AND CODING”, Cambridge University Press (2004).
9. F.J. MacWilliams, N.J.A. Sloane, “THE THEORY OF ERROR-CORRECTING CODES”, North Holland Publishing Co. (1977).
10. A. Menezes, P. van Oorschot, S. Vanstone, “HANDBOOK OF APPLIED CRYPTOGRAPHY”, CRC Press (1996).
11. R.A. Mollin, “RSA AND PUBLIC-KEY CRYPTOGRAPHY”, Chapman and Hall/CRC (2003).
12. M. Stamp, R.M. Low, “APPLIED CRYPTOANALYSIS: BREAKING CIPHERS IN THE REAL WORLD, Wiley Publishing Inc. (2007).
13. D.R. Stinson, “CRYPTOGRAPHY — THEORY AND PRACTICE”, CRC Press (1995).
14. C. Swenson, “MODERN CRYPTANALYSIS”, Wiley Publishing Inc. (2008).
15. R. Wobst, “CRYPTOLOGY UNLOCKED”, Wiley Publishing Inc. (2007).

