Algebra per codici e crittografia

Luca Giuzzi

Anno Accademico 2013–14

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).