Algebra per codici e crittografia

Luca Giuzzi

Anno Accademico 2010–11

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. Problemi fondamentali: sicurezza, integrità, autenticità, correttezza.
2. Gruppi ciclici e gruppi di permutazioni.
3. Algoritmi basati sul logaritmo discreto: Diffie-Hellman, El-Gamal.
4. Aritmetica modulare e elementi di teoria dei numeri.
5. RSA.
6. Campi finiti.

7. La costruzione di AES.
8. Elementi di crittoanalisi.
9. Curve ellittiche: il gruppo dei punti e le applicazioni alla crittografia.
10. Schemi per key-escrow.
11. Protocolli a conoscenza zero.
12. Codici correttori a blocchi.
13. La costruzione dei codici ciclici; motivazioni.
14. Codici di Reed–Solomon; trasformata discreta.
15. Conclusioni.

3 Bibliografia

▷ Testi principali

1. M.W. Baldoni, C. Ciliberto, G.M. Piacentini Cattaneo, "Aritmetica, crittografia e codici", Springer-Verlag Unitext **24** (2006).
2. L. Giuzzi, "Codici correttori", Springer-Verlag Unitext **25** (2006).

▷ Testi consigliati

1. C. Cid, S. Murphy, M. Robshaw, "Algebraic aspects of the Advanced Encryption Standard", Springer-Verlag (2006).
2. M.J. Hinek, "Cryptoanalysis of RSA and its variants", Chapman and Hall/CRC (2010).
3. N. Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag (1994).
4. N. Koblitz, "Algebraic Aspects of Cryptography", Springer-Verlag (1996).
5. A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press (1996).

6. R.A. Mollin, "RSA and Public-Key cryptography", Chapman and Hall/CRC (2003).

7. D.R. Stinson, "Cryptography — Theory and practice", CRC Press (1995).