CR2 Crittografia 2

A.A. 2004/2005

Prof. Marco Pedicini

Crittografia Applicata

1. Crittografia Classica

- Crittosistemi di base: cifratura per sostituzione, cifratura per traslazione (shift), cifratura affine, cifratura di Vigenère, cifratura di Hill, cifratura per permutazione. Cifratura a flusso (sincrona e asincrona), Linear feedback shift registers (LFSR), Cifrario autokey. Cifrari prodotto.
- Crittoanalisi di base: classificazione degli attacchi; crittoanalisi per i cifrari affini; crittoanalisi per la cifratura a sostituzione (analisi delle frequenze); crittoanalisi per la cifratura di Vigenère: Kasiski test, indice di coincidenza; crittoanalisi del cifrario di Hill; crittoanalisi degli LFSR.

2. Applicazione della Teoria di Shannon alla crittografia

- Sicurezza dei cifrari: sicurezza computazionale, sicurezza dimostrabile, sicurezza incondizionata.
- Richiami di calcolo delle probabilità: variabili aleatorie discrete, probabilitá congiunta, probablitá condizionata, variabili aleatorie indipendenti, teorema di Bayes.
- Variabili aleatorie associate a crittosistemi. Sistemi di cifratura a sicurezza perfetta. Crittosistema di Vernam.
- Entropia. Codici di Huffman. Spurious Keys e Unicity distance.

3. Cifrari a blocchi

- Schemi di cifratura iterativi; Reti di Sostituzione-Permutazione (SPN);
- Crittoanalisi lineare per SPN: Piling-Up Lemma, approssimazione lineare di S-boxes, attacchi lineari a S-boxes;
- Crittoanalisi differenziale per SPN;
- Cifrari di tipo Feistel; DES: descrizione e analisi; AES: descrizione; Cenni sui campi finiti: operazioni su campi finiti, algoritmo di Euclide generalizzato per il calcolo del mcd e degli inversi;
- Modi operativi per i cifrari a blocchi.

4. Funzioni Hash e Codici per l'autenticazione di messaggi

- Funzioni di hash e integrità dei dati.
- Funzioni di hash sicure: funzioni one-way o resistenza alla controimmagine, resistenza alla seconda controimmagine, resistenza alla collisione.
- Il modello dell'oracolo random: funzioni di hash ideali, proprietà di indipendenza.

- Algoritmi randomizzati, applicazioni del modello dell'oracolo.
- Criteri di sicurezza: collisione sul problema della seconda controimmagine, collisione sul problema della controimmagine.
- Funzioni di hash iterate; la costruzione di Merkle-Damgøard.

Testi consigliati

[1] Stinson, D. R., *Cryptography: Theory and Practice, 2nd edition*. Chapman & Hall/CRC, (2002).

Bibliografia supplementare

[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*. CRC press, (1997).
[3] Song Y. Yan, *Number Theory for Computing*. Springer, (2002).
[4] Neal Koblitz, *Algebraic Aspects of Cryptography*. Springer, (1998).
[5] Neal Koblitz, *A Course in Number Theory and Cryptography* . Springer, (1994).
[6] Bruce Schneier, *Applied Cryptography*. Wiley, (1996).
[7] Niels Ferguson, Bruce Schneier, *Practical Cryptography*. Wiley, (2003).
[8] Ross Anderson, *Security Engineering*. Wiley, (2001).

Modalità d'esame

- valutazione in itinere ("esoneri")		☐ SI	■ NO
- esame finale	scritto	■ SI	☐ NO
	orale	☐ SI	■ NO
- altre prove di valutazione del profitto (meglio descritte sotto)		■ SI	☐ NO

L'esame consiste di tre parti: l'esposizione di una tesina, un esame scritto e un progetto di programmazione.

Gli argomenti della tesina e del progetto di programmazione devono essere concordati con il docente.

La tesina consiste nell'esposizione della descrizione di un sistema di cifratura e degli eventuali attacchi conosciuti. Il progetto di programmazione consiste nella implementazione delle funzioni di cifratura, e di decifratura del crittosistema e nella implementazione di uno degli attacchi noti. Può essere eseguito in un linguaggio a scelta dello studente tra Java, C, C++, Mathematica.

Il progetto e la discussione della tesina possono essere presentati prima o dopo il superamento dello scritto.

La prova orale é prevista per riparare le insufficenze lievi allo scritto.