CR2 Crittografia 2

A.A. 2002/2003

Prof. Alberto Berretti e Prof. Marco Pedicini

Crittografia Applicata

1. Crittografia Classica

- Crittosistemi di base: cifratura per traslazione (shift), cifratura per sostituzione, cifratura affine, cifratura di Vigenère, cifratura di Hill, cifratura per permutazione, cifratura a flusso. 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;

2. Teoria di Shannon

- Entropia, entropia relativa, cifrari perfetti (codice Vernam).

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; DES: descrizione e analisi; AES: descrizione; Modi operativi per i cifrari a blocchi.

4. Cifrari a blocchi

- 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: funzioni di hash ideali.
- Algoritmi che utilizzano il 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; Algoritmo di Hash Sicuro (SHA-1).
- Codici di Autenticazione (MAC): codici di autenticazione nidificati (HMAC); MAC incodizionatemente sicuri.

Testi consigliati

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

Bibliografia supplementare

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 due parti: un esame scritto e un progetto di programmazione.

Il soggetto del progetto di programmazione deve essere concordato con uno dei docenti e deve essere eseguito in un linguaggio a scelta dello studente tra Java, C, Mathematica.

Il progetto può essere presentato prima o dopo il superamento dello scritto.

La prova orale é prevista per riparare le insufficenze lievi.