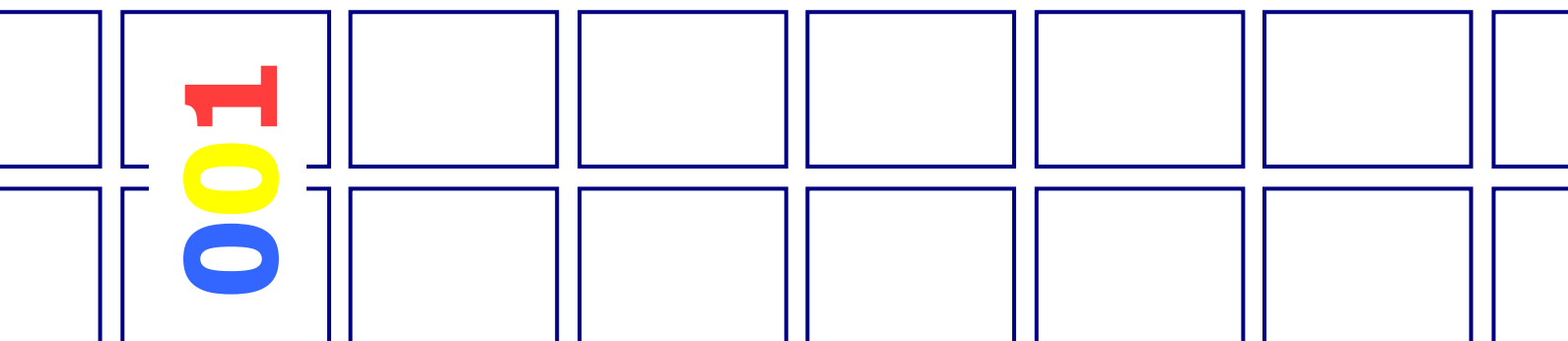


Andrea Pasquinucci



Aspetti di Crittografia Moderna

Da DES alla Crittografia Quantistica



Aspetti di Crittografia Moderna

Da DES alla Crittografia Quantistica

Andrea Pasquinucci

Comitato Tecnico Scientifico



**Associazione Italiana per la
Sicurezza Informatica**

CLUSIT

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.

Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Nell'ambito della Sicurezza Informatica, i soci del CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

Copyright e Disclaimer

Copyright © 2004 Andrea Pasquinucci.

Copyright © 2004 CLUSIT

This work is licensed to Clusit Members only under the Creative Commons Attribution-Non-Commercial- NoDerivs License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/2.0> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

L'obiettivo di questo documento è quello di fornire un'informazione aggiornata e precisa. Qualora dovessero essere segnalati degli errori, nei limiti del possibile, si provvederà a correggerli.

L'autore e Clusit - Associazione Italiana per la Sicurezza Informatica non assumono alcuna responsabilità per quanto riguarda le informazioni contenute nel presente documento.

- Il contenuto non può essere necessariamente esauriente, completo, preciso o aggiornato.
- Il contenuto è talvolta riferito ad informazioni reperite sulla Rete e sia l'autore che Clusit Associazione Italiana per la Sicurezza Informatica non assumono alcuna responsabilità.
- Il contenuto non costituisce un parere di tipo professionale o legale.
- I nomi propri di prodotti e aziende ed i loghi sono esclusiva dei rispettivi proprietari.

Presentazione del Presidente del CLUSIT

La crittografia è, in questo momento, lo strumento più formale e, in relazione a tutta una serie di attacchi informatici, il più efficace di cui dispone la nostra comunità. Una conoscenza anche non approfondita delle leggi che regolano questa disciplina e dei suoi principali risultati, dovrebbe oggi essere parte del bagaglio culturale di ogni professionista della sicurezza informatica. Per il suo aspetto particolarmente rigoroso e formale però la crittografia non è facilmente accessibile a molti, che memori delle fatiche spese, a suo tempo, sui libri di matematica e algebra si mantengono ad una opportuna distanza da questa disciplina, nutrendo al tempo stesso una notevole ammirazione per i risultati che periodicamente i crittografi ci propinano.

Il presente contributo nasce con l'obiettivo principale di consentire proprio a queste persone di avvicinarsi al modo della crittografia e carpirne i suoi segreti. Per svolgere questa missione il CLUSIT ha deciso di chiedere ad Andrea Pasquinucci (socio CLUSIT) e persona con un notevole bagaglio tecnico-scientifico (in settori però del tutto estranei alla crittografia, o meglio che per ora sembrano esserlo), di raccontarci la crittografia a modo suo.

Ne è uscito questo contributo, originale nell'impostazione che sicuramente lo differenzia da tutti i testi di crittografia. In questo testo Andrea non si dilunga in noiose spiegazioni di dettagli implementativi di algoritmi e protocolli, ovviamente fondamentali per chi è interessato alla loro implementazione ma decisamente superflui per chi non ha questo interesse, e riesce a mantenere l'esposizione degli argomenti trattati ad un ottimo livello di astrazione, consentendo al lettore di cogliere gli aspetti e i principi di riferimento, e quindi cogliere il perché di certe scelte.

Sfruttando poi la formazione di Fisico di Andrea, abbiamo osato quello che sinora, credo, nessuno in Italia ha anche solo tentato di fare. Un testo divulgativo sulle nuove frontiere della crittografia, che vedono una convergenza e fusione tra i principi della crittografia classica e la meccanica quantistica, per dare origine ad una disciplina fortemente innovativa quale la crittografia quantistica.

Anche in questo caso il testo è particolarmente introduttivo e riesce a far cogliere gli aspetti e i principi fondamentali senza cadere in divagazioni o descrizione di dettagli superflui.

Ovviamente non poteva mancare anche un accenno ai calcolatori quantistici, che in questo momento sono la principale spina nel fianco della crittografia asimmetrica, ed il cui avvento avrebbe un effetto davvero rivoluzionario sull'intero settore ICT.

In sostanza un testo interessante, dove l'aspetto divulgativo è particolarmente curato senza scadere nell'approssimazione o pressapochismo. Un viaggio nella crittografia a partire dal V secolo a.c. per arrivare ad un futuro che non sappiamo ancora se ci sarà.

Non ci resta che consigliarne la lettura a tutti i nostri soci, che sicuramente sapranno apprezzarlo, sia che conoscano o non conoscano già la disciplina trattata.

Buona Lettura

Prof. Danilo Bruschi

Abstract

In questo documento viene fatta una breve rassegna su vari aspetti della Crittografia moderna. Partendo dai principali elementi teorici della crittografia del XX secolo, si passa a DES, AES, RSA per poi dare uno sguardo a cosa potrebbe succedere nel prossimo futuro e finire considerando alcuni tra gli aspetti più innovativi provenienti dalla ricerca ma che ormai si affacciano all'implementazione commerciale, quale la Crittografia Quantistica.

L'Autore

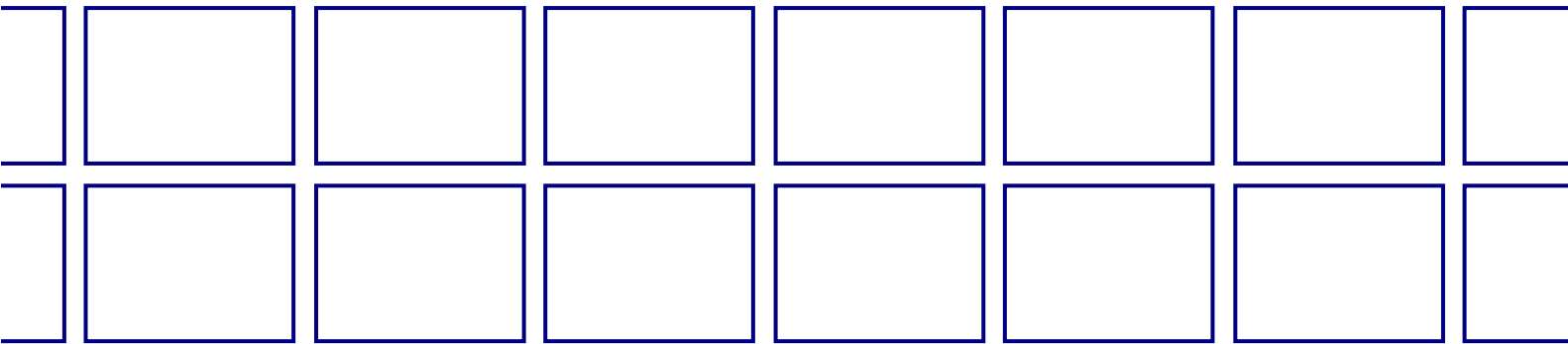
Andrea Pasquinucci

PhD in Fisica, membro del Comitato Tecnico Scientifico CLUSIT. E' un esperto in Sicurezza Informatica e si occupa prevalentemente di crittografia, di sicurezza delle reti e dei sistemi operativi. Con un esteso background di ricerca universitaria all'estero ed in Italia, partecipa a progetti di ricerca finanziati dall'Unione Europea ed insegna in corsi universitari e di specializzazione. Svolge attività professionale e di consulenza sia presso aziende che per fornitori di servizi di sicurezza informatica e telecomunicazioni.

Indice

| | |
|---|----|
| CLUSIT..... | 2 |
| Copyright e Disclaimer..... | 2 |
| Presentazione del Presidente del CLUSIT..... | 3 |
| Abstract..... | 4 |
| L'Autore..... | 4 |
| 0.1 Introduzione..... | 7 |
| 0.2 Crittografia non sempre vuol dire Sicurezza..... | 8 |
| 0.3 La Crittografia è difficile..... | 9 |
| PARTE 1 – ALGORITMI DI CRITTOGRAFIA | 11 |
| 1.1 Una breve regressione storica..... | 11 |
| 1.2 Elementi di base di Crittografia..... | 16 |
| 1.2.1 Il Cifrario di Cesare..... | 17 |
| 1.2.2 One-Time-Pad..... | 18 |
| 1.2.3 Algoritmi Moderni..... | 20 |
| 1.2.4 Tipi di attacchi..... | 22 |
| 1.3 I Principali Algoritmi..... | 24 |
| 1.3.1 Algoritmi Simmetrici..... | 24 |
| 1.3.2 DES..... | 26 |
| 1.3.3 AES..... | 29 |
| 1.3.4 Algoritmi Asimmetrici..... | 30 |
| 1.3.5 RSA..... | 32 |
| 1.3.6 Algoritmi di Hash (Impronte)..... | 34 |
| PARTE 2 – ALGORITMI E PROTOCOLLI CRITTOGRAFICI OGGI E DOMANI..... | 39 |
| 2.1 La Sicurezza dei Principali Algoritmi..... | 39 |
| 2.2 Il Prossimo Sviluppo degli Algoritmi Crittografici..... | 43 |
| 2.3 Protocolli ed applicazioni, da oggi a domani..... | 45 |
| 2.3.1 Algoritmi e Protocolli..... | 45 |
| 2.3.2 Certificati Digitali, Certification-Authorities e Web..... | 47 |
| 2.3.3 Problemi Aperti ed Applicazioni..... | 49 |
| PARTE 3 – LA CRITTOGRAFIA QUANTISTICA | 55 |
| 3.1 Perché la Fisica Quantistica..... | 55 |
| 3.2 Gli Elaboratori Quantistici e la Sicurezza Informatica..... | 56 |

| | |
|---|----|
| 3.3 La Crittografia Quantistica | 58 |
| 3.3.1 I Principi Generali..... | 59 |
| 3.3.2 La Fisica di Base..... | 62 |
| 3.3.3 Il Protocollo BB84..... | 62 |
| 3.3.4 Eavesdropping..... | 66 |
| 3.3.5 Error Correction e Privacy Amplification..... | 66 |
| 3.4 Problemi di Gioventù | 68 |
| Appendice A: Breve introduzione a OpenPGP..... | 71 |
| Appendice B: Principi di funzionamento di un elaboratore quantistico..... | 77 |
| Bibliografia Essenziale..... | 81 |



CLUSIT Associazione Italiana per la Sicurezza Informatica
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO