Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino
1859

Telsy
A TIM ENTERPRISE BRAND

DISMA

Applicazioni tecnologiche della crittografia

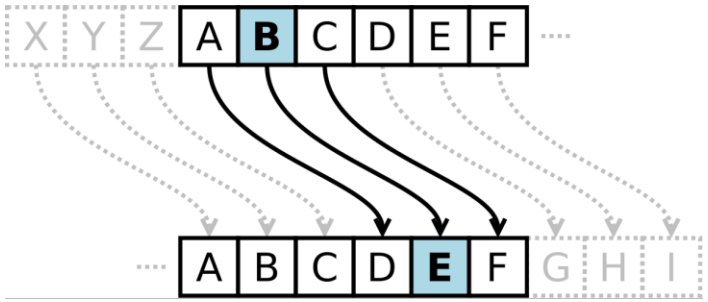
La cybersecurity

01 Un panoramica storica

02 Le applicazioni della crittografia

03 Tra la teoria e la pratica

Crittografia: è una lunga storia…



Cifrario di Cesare
(I sec. a.C.)

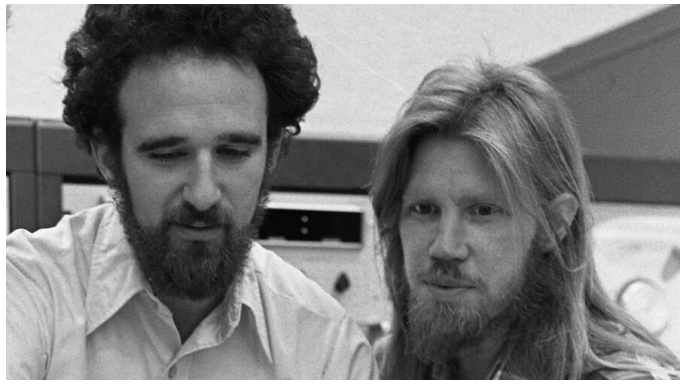
Disco cifrante di Leon Battista Alberti
(XV sec.)

Macchina Enigma
(~1930)

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Crittografia: è una lunga storia…

Purple Machine
(~1940)



Scambio chiave Diffie-Hellman
(1976)

AES
(2001)

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Le applicazioni della crittografia

Gli algoritmi e i protocolli crittografici permettono di garantire

- **Confidenzialità**
- **Integrità**
- **Autenticità**
- **Non ripudio**

in un ampio spettro di scenari applicativi

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

I molteplici usi della crittografia

Pagamenti elettronici

App messaggistica

Blockchain

Cloud

Digital wallet

Telefonia

Telsy | A TIM ENTERPRISE BRAND

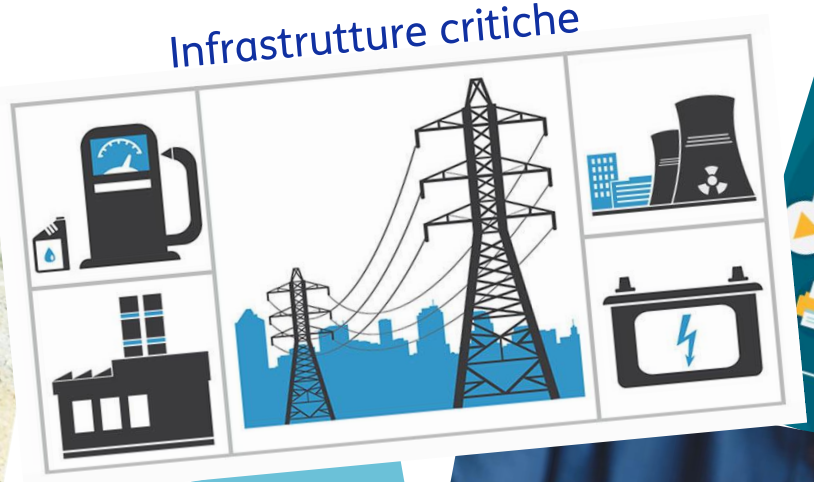
Gruppo TIM - Uso Interno - Tutti i diritti riservati.

I molteplici usi della crittografia

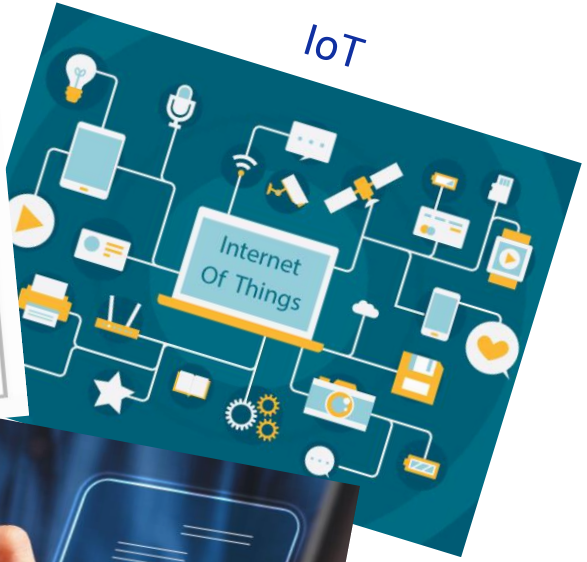
Protocolli VPN

Difesa

Infrastrutture critiche



IoT



Automotive

Voto elettronico

Firma digitale

Telsy | A TIM ENTERPRISE BRAND

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

E un suo abuso

Il celebre ransomware LOCKBIT permette all'attaccante di cifrare tutti i dati presenti sul dispositivo infettato.

Il pagamento del riscatto permette di ottenere la chiave crittografica necessaria per la decifratura delle informazioni

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Tra la teoria e la pratica

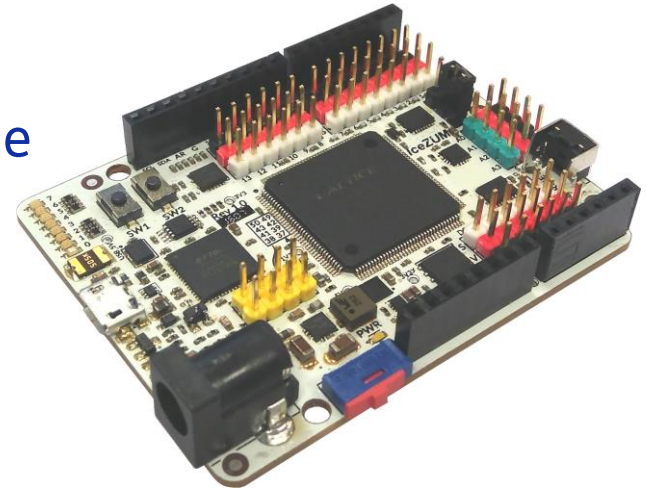
La definizione teorica dell'algoritmo crittografico deve essere seguita dalla sua implementazione

Implementazioni Software

- ✓ Semplicità di sviluppo
- ✓ Costi inferiori
- ✓ Maggiore flessibilità

Implementazioni Hardware

- ✓ Maggiore sicurezza
- ✓ Migliori prestazioni
- ✓ Elevata specializzazione

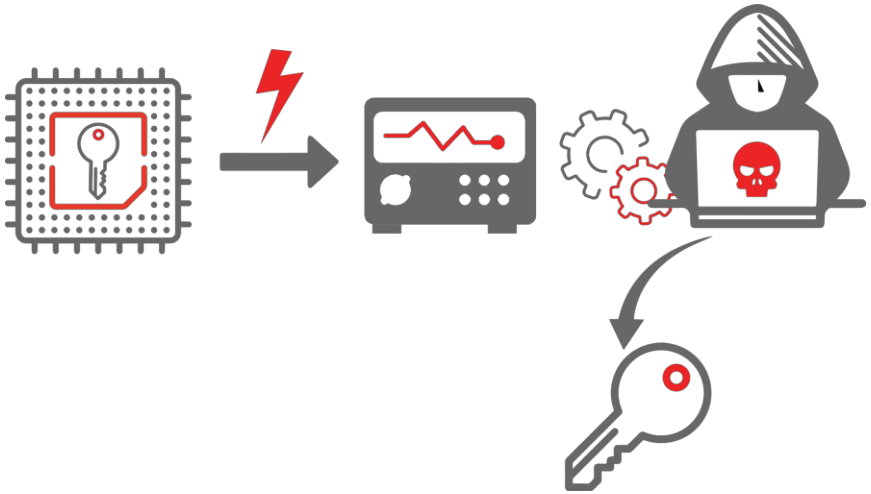


L'obiettivo principale è un giusto **equilibrio tra sicurezza, prestazioni e costi**, variabile in base allo scenario applicativo

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Side-channel

Side-channel attacks: attacchi che mirano a recuperare segreti crittografici sfruttando il leakage di informazioni del dispositivo durante lo svolgimento di operazioni crittografiche.



- **Timing** attacks
- **Power analysis** attacks
- **Cache** attacks
- **Electromagnetic** attacks
- **Optical** attacks

Alcuni attacchi richiedono accesso fisico al dispositivo, altri possono essere fatti da remoto.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Side-channel

Side-channel attacks: attacchi ch… …i crittografici sfruttando il leakage di informazio… …volgimento di operazioni crittografiche.

- **Timing** attacks
- **Power** …
- …**gnetic** attacks
- **Optical** attacks

Alcuni atta… …esso fisico al dispositivo, altri possono essere fatti da remoto.

Is Your Bluetooth Chip Leaking Secrets via RF Signals?

Optical Cryptanalysis: Recovering Cryptographic Keys from Power LED Light Fluctuations

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

C	R	A	C	K	I	N	G

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	A	C	K	I	N	G

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	A	C	K	I	N	G

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

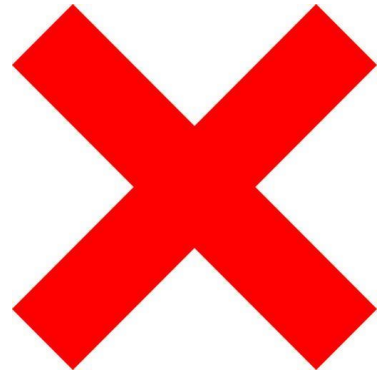
Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

≠

C	R	A	C	K	I	N	G



Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	Y	P	T	O	2	?

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	Y	P	T	O	2	?

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	Y	P	T	O	2	?

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	Y	P	T	O	2	?

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	Y	P	T	O	2	?

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	Y	P	T	O	2	?

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

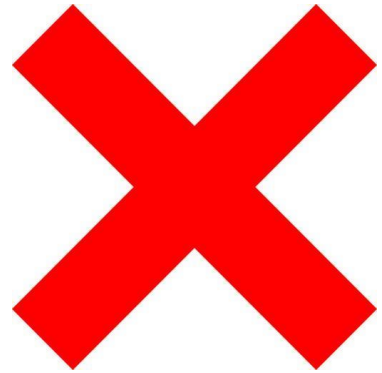
Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

=

C	R	Y	P	T	O	2	?



Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Un esempio: comparazione di stringhe

In molti linguaggi di programmazione sono presenti funzioni per la comparazione di stringhe che **non** sono **constant-time**

C	R	Y	P	T	O	1	!

C	R	Y	P	T	O	2	?

Timing side-channel attack

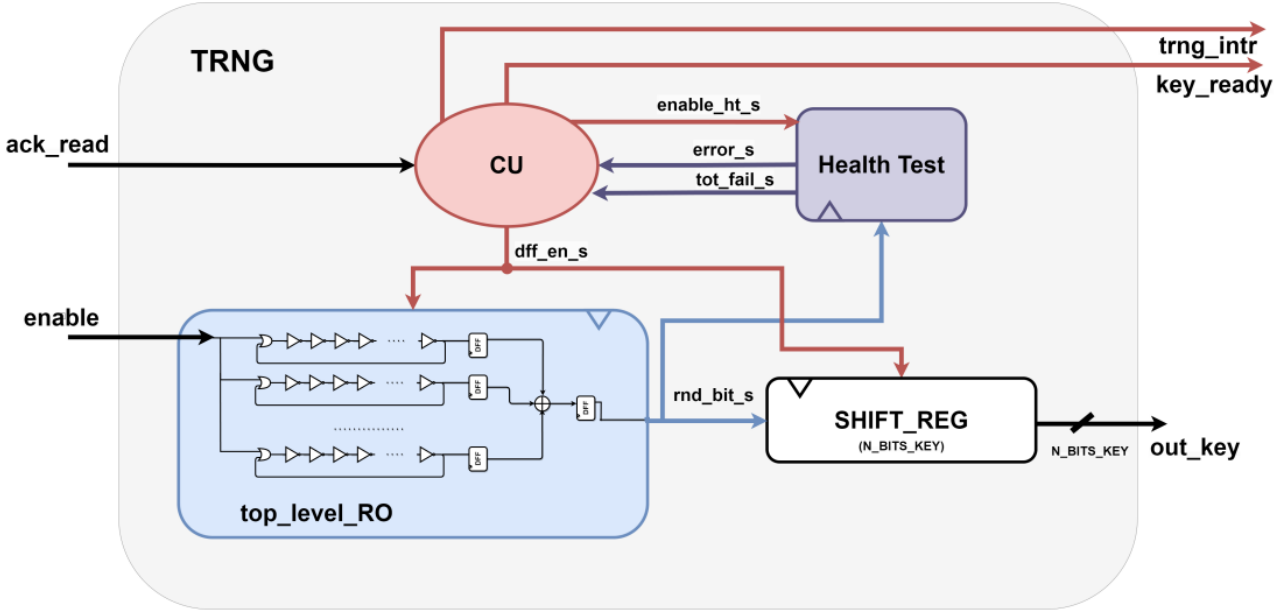
Gruppo TIM - Uso Interno - Tutti i diritti riservati.

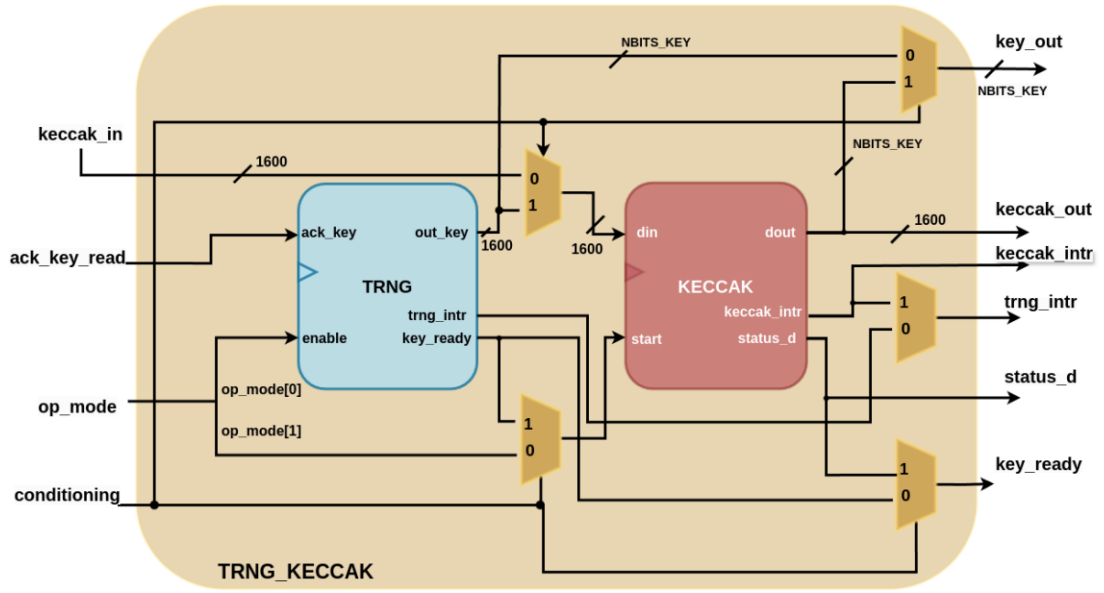
Il random

In teoria:

$$x \xleftarrow{\$} \{0,1\}^k$$

Nella pratica:



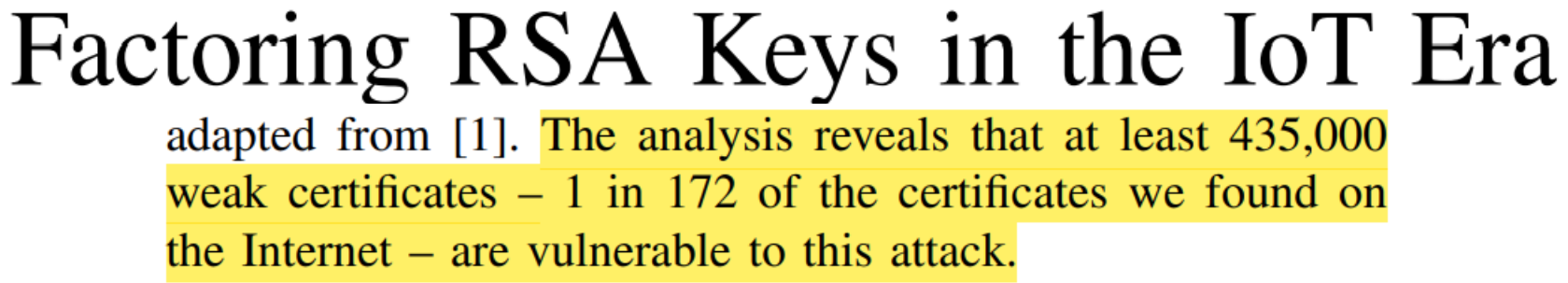


V.Piscopo, Design of a true random number generator for post-quantum cryptography., Rel. G. Masera, M. Martina, A. Dolmeta. Politecnico di Torino, Corso di laurea magistrale in Ingegneria Elettronica (Electronic Engineering), 2024

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Il random

Materiale random di scarsa qualità (**bassa entropia**) **compromette completamente la sicurezza** di un algoritmo crittografico.



Factoring RSA Keys in the IoT Era

adapted from [1]. The analysis reveals that at least 435,000 weak certificates – 1 in 172 of the certificates we found on the Internet – are vulnerable to this attack.

Per mitigare tali problematiche si ricorre a:

- True Random Number Generators (**TRNG**)
- Quantum Random Number Generators (**QRNG**)
- Test statistici

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Conclusioni

- La crittografia vanta una **lunga e ricca storia**
- **Molteplici ambiti di applicazione** possibili per questa tecnologia
- L'implementazione di algoritmi crittografici richiede **competenze matematiche, informatiche ed elettroniche**
- Una corretta valutazione di tutti gli **aspetti implementativi** è fondamentale per la sicurezza degli schemi crittografici

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Grazie.

marco.rinaudo@telsy.it

CrypTO Conference 22 / 05 / 2025

Gruppo TIM - Uso ...