



Dipartimento di Ingegneria dell'Informazione

Master di I livello in Cybersecurity

Project Work Aziendale

TITOLO ITALIANO.


TITOLO INGLESE.

MARCO BURACCHI

Tutor Accademico: Mario Rossi

Tutor Aziendale: Carlo Bianchi

Anno Accademico 2018-2019

Marco Buracchi: *Titolo italiano.*, Master di I livello in Cybersecurity,
 Creative Commons Attribution-NonCommercial-ShareAlike 4.0
International (CC BY-NC-SA 4.0) , Università di Pisa, Anno Accademico
2018-2019

INDICE

Acronimi	5
----------	---

ELENCO DELLE FIGURE

LISTINGS

ELENCO DELLE TABELLE

*"From camp to camp, through the foul womb of night,
The hum of either army stilly sounds,
That the fixed sentinels almost receive
The secret whispers of each other's watch."*

*"Da campo a campo, nel tetro grembo della notte,
s'avverte appena il brusio di entrambe le armate,
sicché le sentinelle appostate quasi possono udire
i mormorii furtivi delle sentinelle nemiche"*
— Enrico V, William Shakespear

ACRONIMI

AES	Advanced Encryption Standard
ARM	Advanced RISC Machine
BP	Branch Predictor
CNES	Centre National d'Etudes Spatiales
CRT	Chinese Remainder Theorem
CVE	Common Vulnerabilities and Exposures
DBA	Differential Behavior Analysis
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DFIA	Differential Fault Intensity Analysis
DH	Diffie-Hellman
DPA	Differential Power Analysis
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FBA	Fault Behavior Analysis
FIPS	Federal Information Processing Standards
FSA	Fault Sensitivity Analysis
GPS	Global Positioning System
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
LED	Light Emitting Diode
LLC	Last Level Cache

NATO	North Atlantic Treaty Organization
NCSCD₄	National Communications Security Committee Directive 4
NIST	National Institute of Standards and Technology
PICA	Picosecond Imaging Circuit Analysis
PoC	Proof of Concept
QIF	Quantitative Information-flow Analysis
SEA	Safe-Error Attacks
SPA	Simple Power Analysis
SPARK	Spectre-based Password-avoiding Attack to Retrieve Keys
TEMPEST	Transient Electromagnetic Pulse Emanation STandard
TOR	The Onion Router
USB	Universal Serial Bus