



Transizione alla Crittografia Post-Quantum

**DNA - DIREZIONE TECNICA PER L'INFORMATICA, TELEMATICA
E TECNOLOGIE AVANZATE (TELEDIFE)**

Il Ruolo della Crittografia nella Difesa

Ancona, 8 ottobre 2026

AGENDA

- **LA CRITTOGRAFIA NELLA DIFESA**
- **SOGGETTI ISTITUZIONALI**
- **TECNOLOGIE PRINCIPALI**
- **MINACCE**
- **SFIDA POST-QUANTISTICA**

La Crittografia nella Difesa

- è una componente essenziale della sicurezza nazionale:

PROTEGGERE

Comunicazioni

Ordini

Dati Operativi

Piattaforme Militari

Identità Digitali

da

Intercettazione,
Alterazione e
Uso Non Autorizzato

Crittografia: Principali funzioni

FUNZIONE	SCOPO
Riservatezza	Impedire che informazioni militari siano lette da soggetti non autorizzati
Integrità	Rilevare modifiche a messaggi, ordini e dati operativi
Disponibilità / Continuità Operativa	Mantenere comunicazioni sicure anche in ambienti ostili o degradati
Autenticazione	Verificare identità, apparati e provenienza delle comunicazioni
Non ripudio	Collegare determinate operazioni digitali al soggetto che le ha autorizzate

Crittografia: Dove viene impiegata

- Proteggere:

Comunicazioni

**Radio, Satellitari
Navali,
Ordini**

Dati / Informaz. Class.

**Flusso/In Transito
A Riposo**

Piattaforme Militari

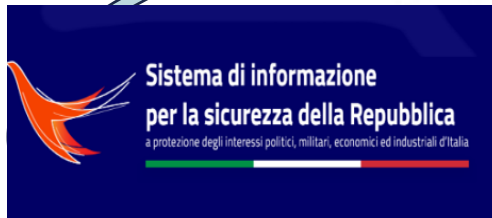
**Comandi e
Aggiornamenti**

Identità Digitali

**Certificati e
Firme Elettroniche**

Soggetti istituzionali

- Il sistema coinvolge più organismi, con competenze differenti:



Unione Europea



Crittografia

Soggetti Istituzionali

Tecnologie Principali

Minacce

Sfida Post-Quantistica

Tecnologie principali

- Le tecnologie impiegate sono molteplici e sono mutate nel tempo:

CRITTOGRAFIA



SIMMETRICA
ASIMMETRICA

Funzioni HASH

Firme Digitali e Certificati

Moduli HW Sicuri

Sistemi Tempest e Protezioni Fisiche

Tecniche Anti-Jamming e Autenticazione di segnali

Un fattore importante: gestione delle chiavi

- In un sistema militare, spesso la **gestione delle chiavi** è più critica dell'algoritmo stesso.
- Immaginate Numero elevato di terminali (es. 1.000) e una rete distribuita.
- Bisogna stabilire:



- ⇒ chi la può possedere;
- ⇒ quando diventa valida;
- ⇒ quando scade;
- ⇒ come viene distribuita;
- ⇒ come viene sostituita;
- ⇒ come viene revocata;
- ⇒ cosa succede se un apparato viene compromesso;
- ⇒ come impedire che una vecchia chiave permetta di decifrare indefinitamente il traffico futuro.

Si parla quindi di key management e di key lifecycle

Crittografia

Soggetti Istituzionali

Tecnologie Principali

Minacce

Sfida Post-Quantistica

Minacce

- Nel contesto degli attacchi ...
 - ⇒ **invece** di affrontare direttamente **l'algoritmo**, l'attaccante analizza **consumi elettrici, tempi di esecuzione, emissioni elettromagnetiche** o altri **effetti fisici dell'apparato**. La protezione richiede quindi non solo matematica robusta, ma anche hardware, implementazioni e procedure sicure.
- (PNRM Laboratorio SCA finanziato da SEGREDIFESA/DNA e sviluppato da Defence Tech)

Altri rischi comprendono:

- ⇒ **furto o compromissione delle chiavi**
- ⇒ **errori di configurazione**
- ⇒ **apparati o software alterati nella catena di fornitura**
- ⇒ **malware e intrusioni nelle reti**
- ⇒ **personale infedele o non adeguatamente formato**
- ⇒ **raccolta odierna di dati cifrati per decifrarli in futuro**



La sfida post-quantistica

- I futuri calcolatori quantistici potrebbero compromettere buona parte della crittografia asimmetrica tradizionale,
- Il rischio è rilevante per la Difesa perché molte informazioni devono rimanere segrete per molti anni.

La transizione alla crittografia post-quantistica richiede di:

- ⇒ **censire algoritmi, certificati e dipendenze crittografiche;**
- ⇒ **stabilire la durata di segretezza dei dati;**
- ⇒ **progettare sistemi dotati di agilità crittografica;**
- ⇒ **sperimentare algoritmi post-quantistici standardizzati;**
- ⇒ **migrare progressivamente, evitando incompatibilità e nuove vulnerabilità.**



Istituto Nazionale di Fisica Nucleare - Qubit

Sfida Post-Quantistica: Ruolo DNA

- Direzione da cui dipendono le Stazioni Appaltanti
- Nel contesto del Sistema Paese ...

⇒ **Il DNA supporta la Ricerca Applicata mediante il finanziamento del Piano Nazionale di Ricerca Militare (PNRM)**

⇒ Co-finanziamento Difesa – Industria e Accademia volto a stimolare la ricerca di soluzioni innovative dual-use

Esempi virtuosi cofinanziati dalla DNA:

- PNRM «Laboratorio SCA» - Defence Tech;
- PNRM «TEP» (Transport Encrypted Protocol) – bitCorp;
- PNRM SSCUDO (Sistema di Sicurezza Cibernetica Unificato per la Difesa Operativa) – RTI MBDA e LEONARDO

⇒ **Il DNA supporta l'Industria nel contesto internazionale e NATO:**

⇒ Presentazione dei nuovi apparati crittografici presso esposizioni dedicate

La sfida post-quantistica: Eventi



- Organizzato presso la sede della società Qinetiq (Portsmouth, UK) è rivolto agli stakeholder di tutto il settore Tactical Secure Voice (TSV).
- Partecipazione di rappresentanti militari e Agenzie di Sicurezza delle più importanti NATO Crypto Producing Nations (CPN) con le relative industrie Nazionali (tra le quali Francia, Germania, Italia, Spagna, UK e US).
- L'Italia ha partecipato con lo scopo di testare la cifrante CM107E-M (pieno successo) con rappresentanti militari in supporto dell'Industria.

La DNA era presente con TELEDIFE

Crittografia

Soggetti Istituzionali

Tecnologie Principali

Minacce

Sfida Post-Quantistica

La sfida post-quantistica: Eventi



National Cyber Security Centre
a part of GCHQ



Tactical Secure Voice
Cryptographic
Modernisation
Symposium

Interoperability Testing
7th – 14th September 2026

Main Event
15th – 17th September 2026



Hosted at
QINETIQ
Portsmouth Technology Park,
Portsmouth,
United Kingdom

- In questa sessione 2026 sono stati eseguiti test mai svolti nelle sessioni precedenti, maggiormente orientate alla sola verifica dell'interoperabilità Suite B con i protocolli STaC-IS e TSVCIS, in modo da avere contezza anche dell'interoperabilità con Suite A, test di caricamento e gestione chiavi anche in modalità Black Key Fill (BKF).
- I protocolli STaC-IS o TSVCIS, consentono di salvaguardare la comunicazione *voice* dal potenziale attacco dei computer quantistici, a patto che la gestione e la generazione delle chiavi crittografiche a monte avvenga tramite sistemi aggiornati agli standard post-quantum (PQC) promossi dal NIST e dalla NSA

Protocolli Quantun-Resistant già in uso

Crittografia

Soggetti Istituzionali

Tecnologie Principali

Minacce

Sfida Post-Quantistica

La sfida post-quantistica: Esempi

Alcuni apparati cifranti e radio in uso e di prossimo impiego nella Difesa



Crittografia

Soggetti Istituzionali

Tecnologie Principali

Minacce

Sfida Post-Quantistica

DOMANDE?