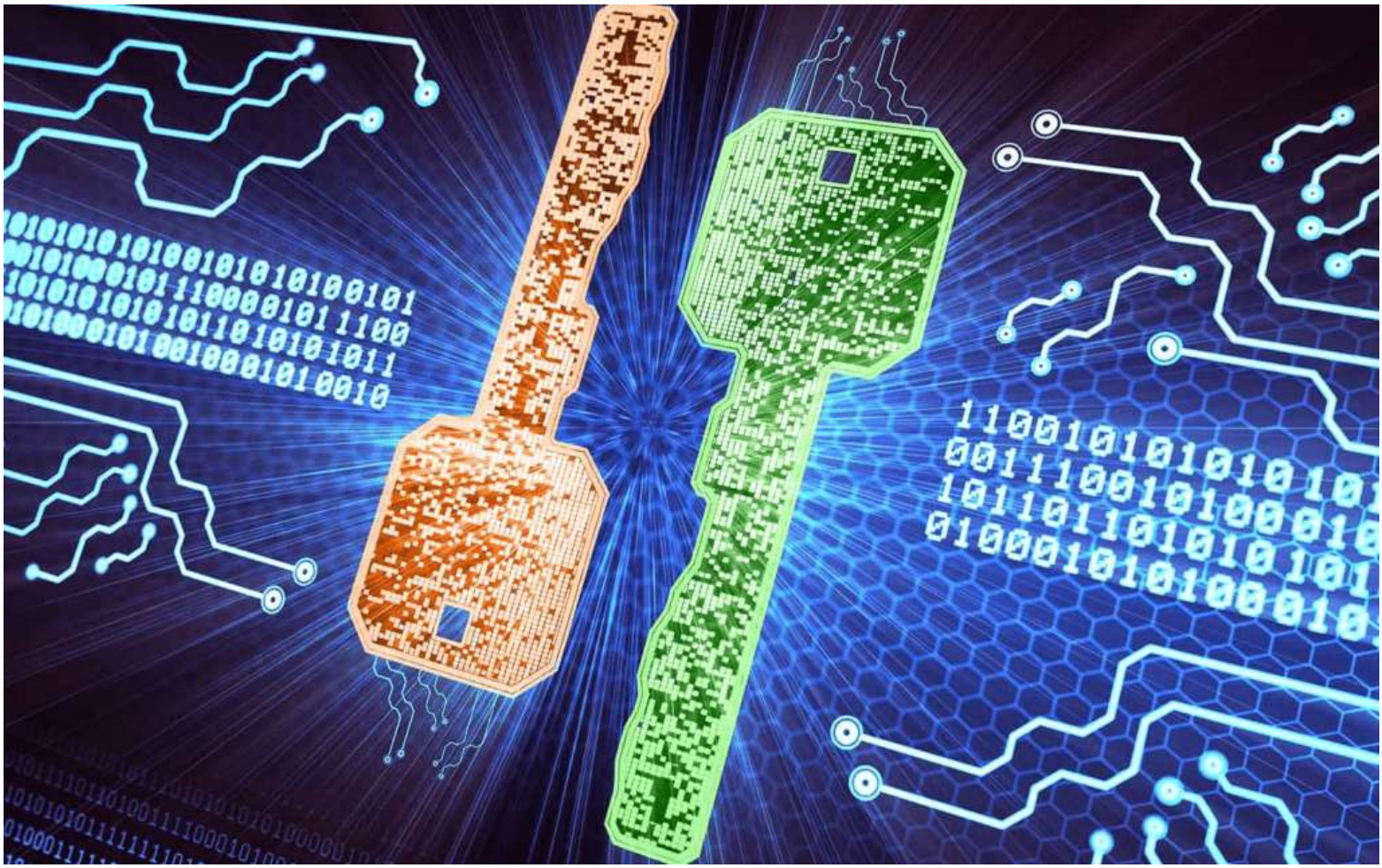
Data Engineering & Security
REAL·T



Corso Executive:
IMPLEMENTAZIONE SICURA DI PRIMITIVE CRITTOGRAFICHE ASIMMETRICHE
(Real-World Cryptography)

Un percorso avanzato dedicato alla progettazione, implementazione e valutazione delle primitive crittografiche asimmetriche nei sistemi reali.
Il corso affronta principi, vulnerabilità e best practice per utilizzare correttamente algoritmi e protocolli crittografici, con particolare attenzione agli errori implementativi che possono compromettere sistemi formalmente sicuri.

Temi principali
Crittografia asimmetrica e gestione delle chiavi
Firma digitale e verifica
Scambio e derivazione delle chiavi
Randomness, nonce e parametri crittografici
Side-channel attack e vulnerabilità implementative
Validazione degli input e gestione degli errori
Implementazioni constant-time
Analisi di casi reali e failure mode
Secure coding per software crittografico
Dalla primitive al protocollo: progettare sistemi robusti

Obiettivo
Comprendere non solo *come funziona* la crittografia moderna, ma soprattutto *come implementarla senza comprometterne le proprietà di sicurezza*.

Per professionisti della cybersecurity, software engineer, security engineer, architect e sviluppatori di sistemi ad alta criticità.

Per informazioni scrivere a:
segreteria@realt.it

Sede di svolgimento: Roma