**Verifica scritta di Sistemi e Reti – Teoria – 3° Trimestre (1)**

Data: 13-03-2025

**Parte 1 - Domande a scelta multipla con Giustificazione (10 punti)**

1. Risposta corretta: C) Principio di Kerkhoffs
   * A) Rivest non ha formulato un principio sulla pubblicità degli algoritmi
   * B) Diffie-Hellman è un algoritmo di scambio chiavi, non un principio
   * D) Shannon non ha enunciato principi sulla segretezza delle chiavi
2. Risposta corretta: A) DAC è più flessibile perché permette agli utenti di modificare i diritti di accesso
   * B) Falso, MAC è più sicuro basandosi su policy definite dall'amministratore
   * C) Falso, DAC è più adatto ad ambienti meno restrittivi
   * D) Falso, con MAC solo l'amministratore gestisce i diritti di accesso
3. Risposta corretta: B) È composta da un master e fino a 7 slave
   * A) Falso, il limite è 8 dispositivi (1 master + 7 slave)
   * C) Falso, master e slave hanno ruoli diversi
   * D) Falso, l'autenticazione è richiesta in Bluetooth
4. Risposta corretta: C) Utilizza una coppia di chiavi correlate (pubblica e privata)
   * A) Falso, usare la stessa chiave è tipico della crittografia simmetrica
   * B) Falso, l'uso di due chiavi rende la crittografia asimmetrica più lenta
   * D) Falso, non richiede una chiave segreta condivisa a priori
5. Risposta corretta: B) È più veloce
   * A) Falso, entrambe possono offrire alta sicurezza con chiavi di dimensioni adeguate
   * C) Falso, la simmetrica richiede la condivisione iniziale della chiave
   * D) Falso, la firma digitale è una funzionalità della crittografia asimmetrica
6. Risposta corretta: B) È una rete perimetrale che ospita i server accessibili dall'esterno
   * A) Falso, la DMZ non contiene solo dispositivi di routing
   * C) Falso, la DMZ è accessibile dall'esterno in modo controllato
   * D) Falso, la DMZ integra e non sostituisce i firewall

**Parte 2 – Vero o Falso con Correzione (10 punti)**

1. Falso. Correzione: In un attacco Man in the Middle, l'attaccante intercetta attivamente la comunicazione e può modificarla.
2. Falso. Correzione: La tecnologia VPN permette di creare connessioni sicure attraverso reti pubbliche come Internet e offre protezione contro gli attacchi Man in the Middle grazie alla crittografia.
3. Falso. Correzione: Le funzioni di hash crittografiche come MD5 e SHA sono progettate per essere difficilmente invertibili (one-way), così da non permettere il recupero del messaggio originale.
4. Falso. Correzione: Nel cifrario a sostituzione di Cesare, le lettere vengono sostituite con altre lettere dell'alfabeto secondo uno spostamento fisso. La trasposizione è un'altra famiglia di cifrari classici.
5. Vero.
6. Vero.

**Parte 3 – Domande aperte e pratiche (20 punti)**

1. L'algoritmo di crittografia simmetrica AES (Advanced Encryption Standard) è basato su una rete a sostituzione e permutazione (SPN). Opera su blocchi di 128 bit usando chiavi di 128, 192 o 256 bit. La sicurezza è garantita da:
   * Struttura iterativa con più round (10, 12 o 14 a seconda della chiave)
   * Operazioni non lineari (S-Box) per aggiungere confusione
   * Diffusione dei bit della chiave e del testo in chiaro su tutto il blocco
   * Derivazione di subkey diverse per ogni round

Un potenziale punto debole è la lunghezza fissa dei blocchi che rende AES vulnerabile ad attacchi basati sul riutilizzo della stessa chiave (es. attacchi a blocchi correlati). Inoltre chiavi troppo corte (es. 128 bit) potrebbero essere violate con attacchi a forza bruta in futuro con calcolatori quantistici.

1. Esempio di architettura di rete sicura con DMZ:
2. Internet <---> Firewall esterno <---> DMZ <---> Firewall interno <---> LAN
   * La DMZ contiene server web, email, DNS esposti in modo controllato
   * Il firewall esterno filtra il traffico da Internet alla DMZ permettendo solo connessioni ai servizi sulla DMZ sulle porte necessarie
   * Il firewall interno restringe ulteriormente l'accesso dalla DMZ alla LAN interna
   * I server nella DMZ non devono poter avviare connessioni verso la LAN

Una VPN può essere usata per collegare sedi remote alla LAN centrale in modo sicuro attraverso Internet. A differenza della DMZ che è una rete fisica separata, la VPN crea tunnel logici criptati. Entrambe aumentano la sicurezza segmentando la rete.

1. Principali attacchi informatici e relative contromisure:
   * Malware (virus, worm, trojan...): antivirus, non aprire allegati sospetti
   * Phishing: controlli anti-spam, formazione utenti, autenticazione multifattore
   * Denial of Service (DoS): firewall, sistemi di rilevamento intrusioni (IDS/IPS)
   * Exploit: patch regolari dei sistemi, hardening, principio del minimo privilegio
   * Man in the Middle: crittografia, VPN, usare protocolli sicuri (HTTPS, SSH...)
   * Password deboli: policy stringenti, usare password manager, autenticazione a più fattori

La sicurezza a più livelli (defense in depth) è cruciale, ancora di più nel wireless dove il mezzo è condiviso. Bisogna combinare:

* + Crittografia robusta (WPA2/WPA3, non WEP)
  + Nascondere SSID, filtrare indirizzi MAC
  + Cambiare password di default, usare PSK robuste
  + Segmentare reti wireless da quelle cablate
  + Tenere aggiornati AP e client, disabilitare WPS
  + Monitorare reti per rilevare access point non autorizzati