Domande Multiple Sicurezza

Scegli l'affermazione sbagliata:
- La caratteristica di permanenza stabilisce che una chiave biometrica non cambia nel tempo
- La caratteristica di permanenza stabilisce il grado di permanenza di una determinata biometria
- La caratteristica di permanenza può determinare la stabilità a breve o a lungo termine di un sistema biometrico
- La caratteristica di permanenza caratterizza il tempo di permanenza necessario all'acquisizione di una determinata biometria [X]

Scegli l'affermazione sbagliata:
- L'identificazione basata su sistemi biometrici si occupa di effettuare il matching "uno a molti" e matching "uno a pochi"
- L'identificazione basata su sistemi biometrici può operare sia su soggetti cooperativi che su soggetti non cooperativi
- L'identificazione basata su sistemi biometrici cerca una corrispondenza all'interno di un database di modelli
- Nessuna delle precedenti [X]

Scegli l'affermazione sbagliata:
- I sistemi biometrici consentono l'identificazione e l'autenticazione di un utente
- I sistemi biometrici possono essere basati su caratteristiche fisiologiche o comportamentali
- I sistemi biometrici sono tipicamente utilizzati per il controllo degli accessi in sedi governative
- Nessuna delle altre tre scelte [X]

Scegli l'affermazione sbagliata:
- L'identificazione/autenticazione è un processo iterativo
- Il processo di Identificazione/autenticazione avviene dopo il processo di Enrollment
- Il processo di Identificazione/autenticazione avviene prima del processo di Enrollment [X]
- Il processo di Identificazione/autenticazione si basa su un template matcher

Scegli l'affermazione sbagliata:
- L'analisi dinamica può portare alla diffusione del malware su altri sistemi mediante la rete
- L'analisi dinamica è tipicamente effettuata utilizzando una modalità di rete chiamata "air-gapped"
- L'analisi dinamica è sempre indipendente dall'analisi statica [X]
- L'analisi dinamica può portare all'infezione del sistema su cui il malware viene eseguito, oltre che dei dati in esso contenuti

Scegli l'affermazione sbagliata:
- La fase di replicazione e propagazione è tipica della maggior parte dei software malevoli
- Tutti i software malevoli presentano obbiettivi di replicazione e propagazione [X]
- La fase di replicazione e propagazione è tipicamente condotta dal malware al verificarsi di determinati eventi o condizioni

Scegli l'affermazione sbagliata:
- L'analisi statica viene di solito effettuata dopo quella dinamica [X]
- L'analisi statica consente di effettuare l'analisi del codice e della struttura di un malware
- Durante l'analisi statica il malware non viene eseguito

Scegli l'affermazione sbagliata:
- L'analisi dinamica consiste nell'esaminare un malware durante la sua esecuzione
- L'analisi dinamica viene di solito effettuata dopo quella statica
- L'analisi dinamica può portare all'infezione del sistema su cui essa viene effettuata
- Nessuna delle precedenti [X]

Scegli l'affermazione sbagliata:
- La codifica in Base64 non consente di processare dati il cui numero di bit non sia multiplo di 24 [X]
- La codifica in Base64 consente di memorizzare o trasferire flussi di bit mediante caratteri stampabili

- La codifica in Base64 processa i dati in blocchi da 24 bit
- La codifica in Base64 opera su blocchi di dati da 6 bit

Scegli l'affermazione sbagliata [+1]:
- L'AES non è un cifrario di Feistel
- Tutte le operazioni usate dall'AES sono facilmente ed efficientemente implementate sia su architetture ad 8 bit che a 32 bit
- Non sono chiari i criteri costruttivi delle S-box per l'AES [X]
- È possibile utilizzare chiavi di 128, 192, 256 per l'AES e la lunghezza del blocco è 128 bit

Scegli l'affermazione sbagliata [+2]:
- Le S-box del DES furono progettate per resistere all'attacco noto poi come Crittoanalisi Differenziale
- Il DES è stato abbandonato come standard a causa del suo avalanche effect [X]
- Il DES è stato abbandonato come standard perché la chiave è troppo corta
- Il DES può essere rotto in meno di una settimana con poche migliaia di euro o anche meno di un giorno

Scegli l'affermazione sbagliata [+1]:
- Il comando dgst ed il comando cmp possono essere usati per verificare se due file portano ad una collisione
- Il comando dgst può essere usato per calcolare lo SHA256 di un file
- Il comando dgst può essere usato in alternativa al comando hmac per calcolare l'HMAC di un file [X]
- Il comando dgst può essere usato per calcolare l'MD5 di più file

Scegli l'affermazione sbagliata [+1]:
- Il comando rand non può essere usato per generare stringhe di caratteri stampabili [X]
- Il comando rand può utilizzare come seme un file arbitrario
- Il comando rand utilizza di default come seme i random bit forniti da /dev/urandom
- Il seme utilizzato dal comando rand può essere anche non specificato

Scegli l'affermazione sbagliata:
- Il Record Protocol si occupa di garantire la compressione, la confidenzialità e l'integrità dei dati.
- Il Record Protocol utilizza gli algoritmi ed i parametri crittografici negoziati attraverso l'handshake protocol
- Il Record Protocol si occupa di garantire l'autenticazione, la compressione, la confidenzialità e l'integrità dei dati [X]

Scegli l'affermazione sbagliata:
- L'Handshake Protocol garantisce alle parti l'interoperabilità tra le diverse implementazioni del protocollo SSL/TSL
- L'Handshake Protocol è utilizzato per imporre alle parti l'esecuzione di un nuovo handshake [X]
- L'Handshake Protocol consente alle parti di negoziare una ciphersuite
- L'Handshake Protocol consente al Server di autenticare il Client

Scegli l'affermazione sbagliata:
- L'Handshake Protocol consente alle parti di negoziare le primitive crittografiche necessarie per la sicurezza della comunicazione
- L'Handshake Protocol consente alle parti di negoziare i parametri necessari per la sicurezza della comunicazione
- L'Handshake Protocol non consente alle parti di autenticarsi [X]
- L'Handshake Protocol consente alle parti di negoziare la versione del protocollo SSL/TSL da utilizzare

Scegli l'affermazione sbagliata:
- SSL/TLS consentono di ottenere i requisiti di autenticazione, confidenzialità ed integrità
- SSL/TLS consentono alle parti di negoziare le primitive crittografiche da utilizzare per la sicurezza dell'informazioni
- SSL/TSL consente al Client di autenticare il Server, ed eventualmente anche al Server di autenticare il Client
- Nessuna delle precedenti [X]

Scegli l'affermazione sbagliata:
- Una CRL contiene i numeri seriali di tutti i certificati che sono stati revocati
- Una CRL è emessa periodicamente da una CA per rendere noti i certificati che sono stati revocati
- Una CRL non contiene i numeri seriali di tutti i certificati che sono scaduti
- Nessuna delle precedenti [X]

Scegli l'affermazione sbagliata:
- Il calcolo della Timestamp Request è basato sull'utilizzo di funzioni hash
- Il calcolo della Timestamp Response è basato sull'utilizzo di funzioni hash e firme digitali
- Il Timestamp Response include un timestamp
- Nessuna delle precedenti [X]

Scegli l'affermazione corretta [+1]:
- I cifrari a sostituzione monoalfabetica sono stati facilmente decifrati usando principalmente un'analisi delle frequenze delle lettere [X]
- I cifrari a sostituzione monoalfabetica sono stati facilmente decifrati usando le raccomandazioni del NIST
- I cifrari a sostituzione monoalfabetica sono stati facilmente decifrati usando semplicemente una ricerca esaustiva nello spazio delle chiavi

Scegli l'affermazione corretta:
- Enigma usava 3 rotori ed un disco per l'involuzione [X]
- Le macchine a rotori sono state inventate da Alan Turing per rompere Enigma
- Ogni rotore Enigma realizza una sostituzione polialfabetica

Scegli l'affermazione corretta:
- Il cifrario one-time pad è impossibile da rompere [X]
- È possibile rompere il cifrario one-time pad se la chiave non è lunga
- Non si sa se esiste un algoritmo efficiente che rompe il cifrario one-time pad

Scegli l'affermazione corretta:
- Le caratteristiche di un sistema biometrico sono: Universalità, Unicità, Permanenza e Catturabilità

Scegli l'affermazione corretta:
- Nel ciclo di vita di un malware le fasi seguono il seguente ordine: Infezione, Quiescenza, Replicazione e Propagazione, Azioni Malevole. [X]

Scegli l'affermazione corretta:
- È possibile effettuare il "resume" di una sessione a patto che il Client e Server abbiano memorizzato i parametri di sessione [X]
- È possibile effettuare il "resume" di una sessione mediante lo scambio di opportune chiavi
- È possibile effettuare il "resume" di una sessione mediante generatori pseudo-casuali

Scegli l'affermazione corretta:
L'i-esima iterazione nel DES è data da:
- $L_i = R_{(i-1)}$ ed $R_i = L_{(i-1)}$ XOR $f(R_{(i-1)}, K_i)$ [X]

Scegli l'affermazione corretta:
- L'algoritmo di decifratura del DES è uguale a quello di cifratura, incluso l'ordine delle sotto chiavi
- L'algoritmo di decifratura del DES è uguale a quello di cifratura, ma l'ordine delle sotto chiavi deve essere invertito e bisogna in aggiunta scambiare la metà destra finale con la metà sinistra
- L'algoritmo di decifratura del DES è uguale a quello di cifratura, incluso l'ordine delle sotto chiavi, ma bisogna in aggiunta scambiare la metà destra finale con la metà sinistra
- L'algoritmo di decifratura del DES è uguale a quello di cifratura, ma l'ordine delle sotto chiavi deve essere invertito [X]

Scegli l'affermazione corretta:
- A partire da una chiave pubblica RSA a 1024 bit è facile recuperare la relativa chiave privata
- A partire da una chiave pubblica RSA a 1024 bit è molto difficile recuperare la relativa chiave privata [X]
- A partire da una chiave pubblica RSA 1024 bit è impossibile recuperare la relativa chiave privata

Scegli l'affermazione corretta:
- La sicurezza della firma RSA e della firma DSS si basano entrambi sulla difficoltà di calcolare logaritmi discreti
- La sicurezza della firma RSA si basa sulla difficoltà di fattorizzare e la sicurezza del DSS sulla difficoltà di calcolare logaritmi discreti [X]
- La sicurezza della firma RSA e della firma DSS si basano entrambi sulla difficoltà di fattorizzare

Scegli l'affermazione corretta:
- La cifratura di un messaggio viene sempre fatta con una singola esponenziazione modulare. La grandezza di un messaggio non è un problema poiché l'operazione viene eseguita in aritmetica modulare.
- RSA viene usata per cifrare il messaggio purché sia meno grande del modulo, altrimenti si divide il messaggio in blocchi di grandezza opportuna e si cifra ogni singolo blocco con RSA.
- Il modulo di RSA viene scelto molto grande, proprio per cifrare messaggi molto grandi. Quindi RSA non può essere usata per messaggi di grandezza maggiore del modulo.
- RSA viene usata per cifrare una chiave scelta casualmente che poi verrà usata per cifrare il messaggio mediante un cifrario simmetrico. [X]

Scegli l'affermazione corretta [+1]:
- I cifrari a chiave pubblica sono utili perché rendono necessari i certificati digitali ed evitano l'anonimia
- I cifrari a chiave pubblica sono utili perché si basano su problemi computazionali impossibili da risolvere efficientemente
- I cifrari a chiave pubblica sono utili perché hanno una sicurezza maggiore rispetto ad AES avendo chiavi di lunghezza maggiore di 256bit
- I cifrari a chiave pubblica sono utili perché risolvono il problema della condivisione di chiavi asimmetriche [X]

Scegli l'affermazione corretta [+1]:
- Il certificato lega l'identità di Alice alla propria chiave pubblica ed emesso da un CA è firmato usando la chiave pubblica cella CA
- Il certificato lega l'identità di Alice alla propria chiave pubblica ed emesso da una CA è firmato usando la chiave pubblica di Alice
- Il certificato che lega l'identità di Alice alla propria chiave pubblica ed emesso da una CA è firmato usando la chiave privata della CA [X]
- Il certificato che lega l'identità di Alice alla propria chiave pubblica ed emesso da una CA è firmato usando la chiave privata di Alice

Scegli l'affermazione corretta:
- Due certificati emessi dalla stessa CA possono avere numeri di serie differenti
- Due certificati emessi dalla stessa CA devono sempre avere numeri di serie differenti [X]
- Due certificati emessi dalla stessa CA devono sempre avere numeri di serie uguali

Scegli l'affermazione corretta:
- Di solito la firma digitale è concatenata all'hash di un file
- Di solito la firma digitale è apposta sull'hash di un file [X]
- Di solito la firma digitale è ricavata a partire dall'hash di un file

Scegli l'affermazione corretta [+2]:
- La firma grafometrica, essendo un caso particolare della firma digitale ha la medesima efficacia probatoria della scrittura privata
- La firma grafometrica è essenzialemnte un'immagine della firma autografa, senza altri rilevanti dati per la non falsificabilità.
- La firma grafometrica, al pari della firma digitale, ha la medesima efficacia probatoria della scrittura privata [X]

Scegli l'affermazione corretta:
- Senza l'utilizzo di una CRL l'unica entità a conoscenza della revoca di un determinato certificato è la CA che ha effettuato la revoca [X]
- Senza l'utilizzo di una CRL le uniche entità a conoscenza della revoca di un determinato certificato sono gli utenti i cui certificati sono stati rilasciati dalla stessa CA che ha effettuato la revoca
- Senza l'utilizzo di una CRL l'unica entità a conoscenza della revoca di un determinato certificato è la CA di livello superiore rispetto a quella che ha effettuato la revoca

Scegli l'affermazione corretta:
- La Certificate Revocation List (CRL) contiene il numero seriale di tutti i certificati revocati [X]
- La Certificate Revocation List (CRL) contiene tutti i certificati con lunghezza della chiave non conforme alle raccomandazioni NIST
- La Certificate Revocation List (CRL) contiene tutti i certificati revocati e scaduti
- La Certificate Revocation List (CRL) contiene chiave pubblica e numero seriale di tutti i certificati revocati e scaduti

Scegli l'affermazione corretta:
- L'autenticazione a due fattori richiede necessariamente la presenza di un cellulare per ricevere messaggi
- L'autenticazione a due fattori richiede necessariamente la presenza di due diverse autenticazioni
- L'autenticazione a due fattori richiede necessariamente la presenza di autenticazioni scelte tra fattori diversi (qualcosa che si sa, qualcosa che si possiede, caratteristiche biometriche) [X]
- L'autenticazione a due fattori richiede necessariamente la presenza di un device con one-time-password

Scegli l'affermazione corretta:
- Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi, uno schema per l'autenticazione, uno schema per la cifratura simmetrica ed uno schema per l'autenticazione del messaggio [X]
- Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi ed uno schema per la cifratura simmetrica
- Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi, uno schema per l'autenticazione, uno schema per cifratura simmetrica, uno schema per l'autenticazione del messaggio ed uno schema per la generazione di numeri pseudocasuali
- Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi, uno schema per l'autenticazione, uno schema per la cifratura simmetrica, ma non uno schema per l'autenticazione del messaggio

Scegli l'affermazione corretta:
- Il Record Protocol consente di ottenere la mutua autenticazione tra le parti
- Il Record Protocol si occupa della segnalazione di situazioni anomale
- I parametri negoziati tramite il Record Protocol sono utilizzati dall'Handshake Protocol
- Nessuna delle precedenti [X]

Scegli l'affermazione corretta:
- I certificati sono importanti nel Code Signing per garantire i diritti di autore
- I certificati sono importanti nel Code Signing per garantire la mancanza di codice malevolo
- I certificati sono importanti nel Code Signing per garantire integrità e provenienza del codice [X]
- I certificati sono importanti nel Code Signing per garantire la qualità del codice e la versione dell'aggiornamento

Scegli l’affermazione corretta:

- Una Key Derivation Function (KDF) consente di derivare la componente pubblica da una coppia di chiavi asimmetriche
- Una Key Derivation Function (KDF) consente di derivare una chiave pseudocasuale a partire da eventi che avvengono nel sistema
- Una Key Derivation Function (KDF) consente di derivare una chiave di cifratura a partire da una PassPhrase [X]

Scegli l’affermazione corretta:

- Se al comando dgst viene passato più di un file, viene calcolato l’hash della concatenazione dei file
- Se al comando dgst viene passato più di un file, viene restituita in output la concatenazione dell’hash dei file
- Se al comando dgst viene passato più di un file, viene restituito in output un messaggio di errore
- Se al comando dgst viene passato più di un file, viene calcolato un hash separato per ciascun file [X]

Scegli l’affermazione corretta:

- Una Time Stamping Authority (TSA) può essere parte di una PKI [X]
- Una Time Stamping Authority (TSA) è usata da una CA per verificare la scadenza di un certificato
- Una Time Stamping Authority (TSA) è usata da un utente per verificare la scadenza di un certificato

Scegli l’affermazione corretta:

- Alcune modalità operative di cifratura sono: ECB, CBC, CFB, OFB, CTR

Scegli l’affermazione corretta:

- L’Enrollment è un processo iterativo

Scegli l’affermazione corretta:

- SHA1 è la più diffusa tra le funzioni hash e non sono noti problemi di sicurezza ad oggi
- Le funzioni di hash SHA-256, SHA-392, SHA-512, raccomandate dal NIST, si basano sull’infallibilità della fattorizzazione
- L’output delle funzioni hash SHA-256, SHA-392, SHA-512 sono 256 bit, 384 bit e 512 bit rispettivamente [X]
- Le funzioni hash SHA-256, SHA-392, SHA-512 raccomandate dal NIST, si basano sull’infallibilità del logaritmo discreto

Scegli l’affermazione corretta:

- Il paradosso del compleanno è utile perché per la sicurezza di tutti è necessario evitare assembramenti e feste nel periodo emergenziale.
- Il paradosso del compleanno è utile per analizzare il tempo necessario per trovare la chiave privata per il DES
- Il paradosso del compleanno è utile per analizzare la difficoltà di invertire le funzioni hash
- Il paradosso del compleanno è utile per analizzare la probabilità di successo di trovare collisioni nelle funzioni hash [X]

Scegli l’affermazione corretta:

- Assumendo che venga utilizzata la codifica in Base64, la stringa binaria (24bit) può essere codificata mediante 4 caratteri stampabili.

Pratica/Domande specifiche:

Si assuma che Alice abbia generato una coppia di chiavi RSA e voglia mandare a Bob la propria chiave pubblica.

- Openssl rsa -in rsaprivatekey.pem -pubout -out rsapublickey.pem

Indicare quale tra le seguenti comandi non consente ad Alice di generare una coppia di chiavi RSA:

- Openssl genrsa -pubout -out rsaprivatekey.pem -passout pass:XXX -aes128 1024 [X]
- Openssl genrsa -out rsaprivatekey.pem -passout pass:XXX -aes128 1024
- Openssl genrsa -out rsaprivatekey.pem -aes128 1024
- Openssl genrsa -out rsaprivatekey.pem -aes128

Siano rsaprivatekey.pem ed rsapublickey.pem rispettivamente le chiavi pubbliche e private di Alice. Indicare quale tra i seguenti comandi consente ad Alice di calcolare una firma per il file testiInChiaro.txt:

- Openssl rsault -sign -pubin -inkey rsapublickey.pem -in testoInchiaro.txt -out rsasign.bin
- Openssl rsault -sign -inkey rsapublickey.pem -in testoInchiaro.txt -pubout -out rsasign.bin
- Nessuna delle precedenti [X]

Siano rsaprivatekey.pem ed rsapublickey.pem rispettivamente le chiavi private e pubbliche di Bob. Indicare quale tra i seguenti comandi consente ad Alice di cifrare un messaggio per Bob:

- Openssl rsault -enctypt -pubin -inkey rsapublickey.pem -in testoInchiaro.txt -out testoCifrato.txt [X]
- Openssl rsault -enctypt -inkey rsapublickey.pem -in testoInchiaro.txt -out testoCifrato.txt
- Openssl rsault -enctypt -inkey rsapublickey.pem -in testoInchiaro.txt -pubout -out testoCifrato.txt

Sia dhparams.pem il file contente i parametri pubblici Diffie-Hellman p e g. Sia dhkey1.pem la chiave privata di Alice e sia dhpub2.pem la chiave pubblica di Bob. Indicare quale tra i seguenti comandi consente ad alice di ottenere una chiave condivisa, a partire dalle informazioni ricevuto da Bob:

- Openssl pkeyutl -derive -inkey -dhkey1.pem -peerkey dhpub2.pem -out segreto1.bin

Indicare quale tra i seguenti comandi consente di generare una stringa pseudocasuale la cui lunghezza sia multipla di 4:

- Nessuna delle precedenti [X]
- Openssl rand -base64 12
- Openssl rand -base64 32
- Openssl rand -base64 19

Siano rsaprivatekey.pem ed rsapublickey.pem rispettivamente le chiavi private e pubbliche di Alcie. Indicare quale tra i seguenti comandi consente ad Alice di calcolare una firma per l'hash SHA-256 per il file testoInChiaro.txt:

- Openssl sa256 -sign rsaprivatekey.pem -out rsasign.bin testoInchiaro.txt [X]
- Openssl sa256 -sign rsaprivatekey.pem -pubout -out rsasign.bin testoInchiaro.txt
- Openssl sa256 -sign -pubin rsaprivatekey.pem -out rsasign.bin testoInchiaro.txt

Si assuma che dhparams1.pem contenga i parametri pubblici Diffie-Hellman p1 e g1. Si assuma inoltre che dhparams2.pem contenga i parametri pubblici Diffie-Hellman p2, g2. Siano Utente1 e Utente2 due utenti.
Scegli l'affermazione sbagliata:

- Sia Utente1 che Utente2 devono usare dhparams1.pem per generare ciascuno la propria coppia di chiavi
- Sia Utente1 che Utente2, devono usare dhparams2.pem per generare ciascuno la propria coppia di chiavi
- Per derivare la propria coppia di chiavi, Utente2 deve usare dhparams2.pem mentre Utente1 deve usare dhparams1.pem rispettivamente [X]

Indica quale tra i seguenti metodi è preferibile come generatore pseudocasuale [+1]:

- Utilizzare la stringa ipod oppure ipad (usate nell'HMAC) come chiave per cifrare il seme, poi cifrare seme+1, poi cifrare seme+2…
- Utilizzare la stringa concatenando X(1), X(2), … dove X(0) = seme X(i) = A*X(i-1)+B mod C, ed A,B,C sono costanti.
- Utilizzare il seme come chiave per AES in counter mode [X]
- Utilizzare la stringa ottenuta concatenando seme, seme+1, seme+2…

Indicare quale dei seguenti metodi è preferibile per memorizzare le password in forma cifrata usando l'AES rispetto agli altri 3 metodi:

- Usando la password come chiave AES e l'account come testo in chiaro

Indica quale tra le seguenti affermazioni è corretta relativamente alla Forward Secrecy:

- La sicurezza dei messaggi cifrati passati non dipende dalla compromissione futura della chiave privata [X]
- La sicurezza dei messaggi cifrati vale anche per il futuro poiché resistenti a tutti gli attacchi
- Fornisce una maggiore sicurezza poiché garantisce anche l'anonimato del mittente
- La confidenzialità dei messaggi cifrati permane anche inoltrandoli ad altri

Indicare quale tra le seguenti affermazioni descrive una corretta generazione dei parametri per la firma digitale RSA [+2]:

- Input L. Generare 2 numeri primi p, q di lunghezza L/2. Calcolare n = pq. Scegliere e tale che gcd(e, (p-1)(q-1)) = 1. Scegliere d come inverso moltiplicativo di e mod (p-1)(q-1). La chiave pubblica è (n, e) e la chiave privata è (n, d)

Indicare quale tra le seguenti descrizioni è corretta relativamente all'accordo su chiavi Diffie-Hellman, dato un numero primo p e un generatore g [+2].

- Alice genera a caso x ed invia g^x mod p. Bob genera a caso y ed invia g^y mod p. La chiave condivisa è g^(xy) mod p.

Indicare quale tra le seguenti affermazioni è corretta data una chiave pubblica RSA (n, e) con chiave privata (n, d):

- La cifratura del messaggio M è data da C = M^e mod n e la decifratura da M = C^d mod n