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

Scegli un'alternativa:

- a. openssl rsautl -encrypt -pubin -inkey rsapublickey.pem -in testoInChiaro.txt -out testoCifrato.txt ✔
- b. openssl rsautl -encrypt -inkey rsapublickey.pem -in testoInChiaro.txt -out testoCifrato.txt
- c. openssl rsautl -encrypt -inkey rsapublickey.pem -in testoInChiaro.txt -pubout -out testoCifrato.txt
- d. Nessuna delle altre tre scelte

Indicare quale tra le seguenti affermazioni non contiene errori.
È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Alcune modalità operative di cifratura sono: ECB, CBC, CFB, OFB, CTR. ✔
- b. Alcune modalità operative di cifratura sono: ECB, CBC, PKCS, OFB, NIST.
- c. Alcune modalità operative di cifratura sono: CBC, MAC, OFB, CTR, HMAC.
- d. Alcune modalità operative di cifratura sono: ECB, CBC, DSS, CTR, EFF.

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Il cifrario one-time pad è impossibile da rompere. ✔
- b. Non si sa se esiste un algoritmo efficiente che rompe il cifrario one-time pad.
- c. Le altre tre scelte sono tutte sbagliate.
- d. È possibile rompere il cifrario one-time pad se la chiave non è lunga.

Indicare quale tra le seguenti affermazioni è corretta relativamente al protocollo per l'accordo su chiavi Diffie-Hellman. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Alice e Bob condividono una chiave privata prima dell'esecuzione del protocollo.
- b. Alice e Bob hanno una chiave pubblica e privata prima dell'esecuzione del protocollo.
- c. Alice e Bob generano una chiave pubblica e privata dopo l'esecuzione del protocollo.
- d. Nessuna delle altre tre scelte. ✔

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. L'*Enrollment* è un processo iterativo.
- b. L'*Enrollment* è un processo ricorsivo.
- c. L'*Enrollment* è un processo in parte iterativo ed in parte ricorsivo. ✖
- d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: L'*Enrollment* è un processo iterativo.

Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Una CRL contiene i numeri seriali di tutti i certificati che sono stati revocati. ✖
- b. Una CRL è emessa periodicamente da una CA per rendere noti i certificati che sono stati revocati.
- c. Una CRL non contiene i numeri seriali di tutti i certificati che sono scaduti.
- d. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è: Nessuna delle altre tre scelte.

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Le caratteristiche di un sistema biometrico sono: Universalità, Univocità, Permanenza e Catturabilità.
- b. Le caratteristiche di un sistema biometrico sono: Universalità, Unicità, Resilienza e Catturabilità.
- c. Le caratteristiche di un sistema biometrico sono: Universalità, Unicità, Permanenza e Catturabilità. ✔
- d. Nessuna delle altre tre scelte.

Indicare quale tra le seguenti motivazioni per cui si firma digitalmente l'hash del messaggio e non direttamente il messaggio è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Per ottenere confidenzialità.
- b. Per permettere la verifica della firma ed evitare l'attacco del compleanno.
- c. Per aggiungere integrità ed autenticazione.
- d. Per migliorare l'efficienza e la sicurezza contro alcuni attacchi. ✔

Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. L'analisi dinamica consiste nell'esaminare un malware durante la sua esecuzione.
- b. L'analisi dinamica viene di solito effettuata dopo quella statica.
- c. L'analisi dinamica può portare all'infezione del sistema su cui essa viene effettuata.
- d. Nessuna delle altre tre scelte. ✔

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Assumendo che venga utilizzata la codifica in Base64, la stringa binaria 010011010110000101101110 può essere codificata mediante 8 caratteri stampabili.
- b. Assumendo che venga utilizzata la codifica in Base64, la stringa binaria 010011010110000101101110 può essere codificata mediante 3 caratteri stampabili.
- c. Assumendo che venga utilizzata la codifica in Base64, la stringa binaria 010011010110000101101110 può essere codificata mediante 4 caratteri stampabili. ✔
- d. Nessuna delle altre tre scelte.

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. 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. ✔
- b. Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi ed uno schema per la cifratura simmetrica.
- c. Una ciphersuite definisce uno schema per l'accordo/scambio di chiavi, uno schema per l'autenticazione, uno schema per la cifratura simmetrica, uno schema per l'autenticazione del messaggio, ed uno schema per la generazione di numeri pseudocasuali.
- d. 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.

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Una Time Stamping Authority (TSA) può essere parte di una PKI.
- b. Una Time Stamping Authority (TSA) è usata da una CA per verificare la scadenza di un certificato.
- c. Una Time Stamping Authority (TSA) è usata da un utente per verificare la scadenza di un certificato.
- d. Nessuna delle altre tre scelte. ✖

Risposta errata.

La risposta corretta è: Una Time Stamping Authority (TSA) può essere parte di una PKI.

Indicare quale tra le seguenti affermazioni è corretta, data una chiave pubblica RSA (n,e) con chiave privata (n,d). È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. La cifratura del messaggio M è data da C = e^M mod n e la decifratura da M = d^C mod n
- b. La cifratura del messaggio M è data da C = M^e mod n e la decifratura da M = C^d mod n ✔
- c. La cifratura del messaggio M è data da C = M^e mod n e la decifratura da M = d^C mod n
- d. La cifratura del messaggio M è data da C = M^e mod n e la decifratura da M = C^d mod phi(n)

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 l'hash SHA-256 per il file *testoInChiaro.txt*. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. openssl sha256 -sign rsaprivatekey.pem -out rsasign.bin testoInChiaro.txt
- b. openssl sha256 -sign rsaprivatekey.pem -pubout -out rsasign.bin testoInChiaro.txt
- c. openssl sha256 -sign -pubin rsaprivatekey.pem -out rsasign.bin testoInChiaro.txt
- d. Nessuna delle altre tre scelte ✖

Risposta errata.

La risposta corretta è: openssl sha256 -sign rsaprivatekey.pem -out rsasign.bin testoInChiaro.txt

Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. L'Handshake Protocol consente alle parti di negoziare le primitive crittografiche necessarie per la sicurezza della comunicazione.
- b. L'Handshake Protocol consente alle parti di negoziare i parametri necessari per la sicurezza della comunicazione.
- c. L'Handshake Protocol non consente alle parti di autenticarsi. ✔
- d. L'Handshake Protocol consente alle parti di negoziare la versione del protocollo SSL/TLS da utilizzare.

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Il DES usa una chiave effettiva di 256 bit e cifra un blocco di 64 bit.
- b. Il DES usa una chiave effettiva di 256 bit e cifra un blocco di 128 bit.
- c. Il DES usa una chiave effettiva di 56 bit e cifra un blocco di 64 bit. ✔
- d. Il DES usa una chiave effettiva di 64 bit e cifra un blocco di 128 bit.

Indicare quale tra le seguenti affermazioni è corretta. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. Il Record Protocol consente di ottenere la mutua autenticazione tra le parti.
- b. Il Record Protocol si occupa della segnalazione di situazioni anomale.
- c. I parametri negoziati tramite il Record Protocol sono utilizzati dall'Handshake Protocol.
- d. Nessuna delle altre tre scelte. ✔

Indicare quale tra le seguenti motivazioni è corretta. E' possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. La sicurezza della firma RSA e della firma DSS si basano entrambi sulla difficoltà di calcolare logaritmi discreti. ✖
- b. Nessuna delle altre tre scelte.
- c. La sicurezza della firma RSA si basa sulla difficoltà di fattorizzare e la sicurezza del DSS sulla difficoltà di calcolare logaritmi discreti.
- d. La sicurezza della firma RSA e della firma DSS si basano entrambi sulla difficoltà di fattorizzare.

Risposta errata.

La risposta corretta è: La sicurezza della firma RSA si basa sulla difficoltà di fattorizzare e la sicurezza del DSS sulla difficoltà di calcolare logaritmi discreti.

Indicare quale tra le seguenti affermazioni è corretta, per la cifratura a chiave pubblica RSA soprattutto quando il messaggio è di grandezza maggiore del modulo. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. 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.
- b. RSA viene usata per cifrare una chiave scelta casualmente che poi verrà usata per cifrare il messaggio mediante un cifrario simmetrico. ✔
- c. 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.
- d. 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.

Indicare quale tra le seguenti affermazioni è sbagliata. È possibile effettuare una sola scelta:

Scegli un'alternativa:

- a. La generazione di bit pseudocasuali in OpenSSL avviene mediante un *Deterministic Random Bit Generator (DRBG)*.
- b. Per la generazione di bit pseudocasuali OpenSSL utilizza di default un CTR DRBG basato su AES a 256 bit.
- c. OpenSSL di dafault utilizza come seme i random bit forniti da */dev/urandom*.
- d. Nessuna delle altre tre scelte. ✔