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

- Il seme utilizzato di default dal comando rand è dato dai bit memorizzati in /dev/random

- Il comando rand può utilizzare come seme soltanto un singolo file alla volta

- Il seme usato dal comando rand deve sempre essere specificato

- Il comando rand può essere usato per generare stringhe di caratteri stampabili

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

- Il Record Protocol non si occupa della segnalazione di situazioni anomale

- I parametri negoziati tramite il Record Protocol sono utilizzati dall’Handshake Protcol

- Nessuna delle altre tre scelte

- Il Record Protocol non consente di ottenere la mutua autenticazione tra le parti

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

- In fase di analisi possono essere estratte generalmente poche stringhe a partire dai programmi legittimi (non malevoli)

- Da un malware compresso (meccanismo di packing) o offuscato possono essere estratte moltissime stringhe

- Nessuna delle altre tre scelte

- Se in seguito all’analisi di un programma vengono individuate molte stringhe, probabilmente il programma è stato offuscato

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

- I disassemblatori consentono di generare il codice assembly a partire dal codice eseguibile (codice macchina)

- I disassemblatori consentono di effettuare l’analisi dinamica black box di un malware

- I disassemblatori consentono di generare codice in un linguaggio di alto livello a partire dal codice eseguibile (codice macchina)

- I disassemblatori consentono di generare codice assembly a partire dal codice in un linguaggio di alto livello

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

- Una Key Derivation Function (KDF) utilizza un salt per derivare una chiave di cifratura

- Nessuna delle altre tre scelte

- Una Key Derivation Function (KDF) consente derivare una chiave di cifratura a partire da una Passphrase

- Una Key Derivation Function (KDF) consente di derivare una chiave di cifratura utilizzando funzioni hash in maniera iterata

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

- L’Handshake Protocol permette alle due parti di calcolare in maniera indipendente la stessa chiave di sessione

- La chiave di sessione in SSL/TLS è calcolata in tre fasi

- La chiave di sessione è calcolata mediante firme digitali

- Il Master Secret è utilizzato dal Record Protocol per garantire la confidenzialità della comunicazione

Siano priv.pem una coppia di chiavi RSA dove priv.pem rappresenta la chiave privata e pub.pem quella pubblica. Indicare il comando che consente di verificare la firma (firma.txt) del file plaid.txt. É possibile effettuare una sola scelta

- openssl pkeyutl -verify -inkey pub.pem -sigfile firma.txt -in plain.txt

- openssl pkeyutl -verify -pubin -inkey pub.pem -sigfile firma.txt -in plain.txt

- Nessuna delle altre tre scelte

- openssl pkeyutl -verify -inkey priv.pem -sigfile firma.txt -in plain.txt

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

Quale dei seguenti non è un tipo di attacco contro le firme digitali

- Chosen Message Attack

- Known Message Attack

- Chosen Cyphertext Attack

- Key-only Attack

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

Alla luce delle conoscenze attuali

- Rompere AES 256 è equivalente computazionalmente a rompere RSA 2048 bit, cioè un algoritmo efficiente per rompere uno dei due può essere usato per rompere l’altro

- Se si trovasse un algoritmo efficiente per rompere RSA 2048 bit allora lo si potrebbe usare per rompere AES 256

- Non si sa se rompere AES 256 e rompere RSA 2048 bit sono due problemi correlati tra loro, cioè un algoritmo efficiente per rompere uno dei due può essere usato per rompere l’altro

- Se si trovasse un algoritmo efficiente per rompere AES 256 allora lo di potrebbe usare per rompere RSA 2048 bit

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

Per lo scambio di chiavi Diffie-Hellman, una scelta corretta (tralasciando considerazioni sulla lunghezza) per il primo p ed il generatore g è:

- p=5 e g=1

- p=7 e g=2

- p=5 e g=2

- p=4 e g=3

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

L’Optimal Asymmetric Encryption Padding (OAEP) viene utilizzato

- Quando si vuole un testo cifrato della stessa lunghezza del testo in chiaro

- Quando si vuole ottenere anche autenticazione oltre alla confidenzialità

- Quando si vogliono evitare gli attacchi CCA

- Quando si vuole ottimizzare la lunghezza del testo cifrato

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

Per lo scambio Diffie-Hellman, una scelta corretta (tralasciando considerazioni sulla lunghezza) per il primo p ed il generatore g:

- p=13 e g=3

- p=7 e g=2

- p=5 e g=3

- p=5 e g=1

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

- Una CA conserva le copie di tutti i certificati che ha emesso

- Una CA conserva le copie dei soli certificati in corso di validità

- Una CA conserva le copie di tutti i certificati in corso di validità

- Una CA conserva le copie di tutti i certificati revocati

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

- È possibile effettuare digitalmente qualunque tipo di documento; nel caso che il documento contenga macro-istruzioni o codice eseguibile, basta cifrarlo prima di firmarlo per avere valore legale

- È possibile firmare digitalmente qualunque tipo di documento, nel caso che il documento contenga macro-istruzioni o codice eseguibile, basta scegliere lo standard opportuno per avere valore legale.

- Non è possibile firmare digitalmente documenti che contengono macro-istruzioni o codice eseguibile

- La firma digitale di documento che contengono macro-istruzioni o codice eseguibile non ha valore legale

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

- Il comando dgst può essere usato per calcolare l’HMAC di più file

- 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 non può essere usato per il calcolo della firma digitale

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

- Una volta che un certificato é stato rilasciato non può essere più modificato

- La revoca di un certificato non richiede una copia del certificato da revocare

- Nella struttura X.509 del certificato revocato viene impostato il flag R

- In un certificato revocato vengono effettuate delle modifiche alla sua struttura

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

Supponiamo che n=pq dove p=17 e q=11 (Sintralascino considerazioni sulla lunghezza). L’esponente pubblico per RSA potrebbe essere

- e=7

- e=5

- e=11

- e=2

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

- L’autenticazione basata su sistemi biometrici opera solo su soggetti cooperativi

- L’autenticazione basata su sistemi biometrici si occupa di effettuare matching “uno ad uno”

- L’autenticazione basata su sistemi biometrici confronta un campione (sample) con un singolo modello archiviato

- L’autenticazione basata su sistemi biometrici si occupa di effettuare matching “uno ad uno” e matching “uno a pochi”

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

- L’Autenticazione si basa su un processo iterativo

- Nessuna delle altre tre scelte

- L’Identificazione avviene prima del processo di Enrollment

- L’Autenticazione avviene su soggetti non cooperativi

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

Supponiamo si scopra un algoritmo polinomiale che da n calcola la funzione di Eulero phi(n)

- Non sono chiare le relazioni con la rottura di RSA

- Si possono calcolare le esponenziazioni in modo efficiente

- Quindi esisterebbe un algoritmo polinomiale che calcola il logaritmo discreto

- Quindi esisterebbe un algoritmo polinomiale che fattorizza

1. 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:

* Per ottenere confidenzialità
* Per permettere la verifica della firma ed evitare l’attacco del compleanno
* Per aggiungere integrità ed autenticazione
* Per migliorare l’efficienza e la sicurezza contro alcuni attacchi

1. Sia KeyA.pem file contenente la coppia di chiavi Diffie-Hellman di Alice. Indicare il comando per estrarre la chiave pubblica a partire da KeyA.pem. è possibile effettuare una sola scelta:

* Openssl pkey -in keyA.pem -pubout -out pubA.pem
* Openssl pkey -in keyA.pem -out pubA.pem
* Openssl pkeyult -in keyA.pem -out pubA.pem
* Nessuna delle altre tre scelte

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

In un cifrario Feistel l’i-esima iterazione può essere descritta come:

* L\_{i+1} = R\_i e R\_{i+1} = L\_i XOR f(L\_{i} XOR R\_i, K\_{i+1})
* L\_{i+1} = R\_i XOR L\_i e R\_{i+1} = L\_{i} XOR f(R\_i, K\_{i+1})
* L\_{i+1} = R\_i e R\_{i+1} = L\_i XOR f(L\_i, K\_{i+1})
* L\_{i+1} = R\_i e R\_{i+1} = L\_i XOR f(R\_i, K\_{i+1})

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

Scegli un’alternativa:

* Utilizzando Base64 per codificare la stringa binaria 01000001010000100100001101000100 sono necessari 6 caratteri stampabili
* Utilizzando Base64per codificare la stringa binaria 001000001010000100100001101000100 sono necessari 8 caratteri stampabili
* Nessuna delle altre tre scelte
* Utilizzando Base64 per codificare la stringa binaria 01000001010000100100001101000100 sono necessari 7 caratteri stampabili

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

* Nessuna delle altre tre scelte
* L’analisi dinamica white box non può portare all’infezione dei sistemi su cui essa viene effettuata
* L’analisi dinamica black box rappresenta un approccio superficiale per la comprensione di un malware
* L’analisi dinamica consiste nell’esaminare un malware prima della sua esecuzione

1. Siano priv.pem ed pub.pem una coppia di chiavi RSA, dove priv.pem rappresenta la chiave privata e pub.pem quella pubblica. Indicare il comando che non consente di calcolare una firma RSA (firma.txt) per l’hash SHA-256 del file plain.txt

È possibile effettuare una sola scelta:

* Openssl dgst -sha256 -sign priv.pem -out firma.txt plain.txt
* Openssl sha256 -sign -pubin priv.pem -out firma.txt plain.txt
* Openssl sha256 -sign priv.pem -out firma.txt plain.txt
* Nessuna delle altre tre scelte

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

Supponiamo che n=pq, dove p=5 e q=7 (si tralascino considerazioni sulla lunghezza). L’esponente pubblico per RSA potrebbe essere:

* e=4
* e=5
* e=9
* e=3

1. siano pub.pem e priv.pem le chiavi pubbliche e private di Alice, rispettivamente. Indicare il comando che consente a Bob di cifrare un messaggio per Alice. È possibile effettuare una sola scelta:

* openssl pkeyutl -encrypt -pubin -inkey pub.pem -in plain.txt -out cipher.txt
* openssl pkeyutl -encrypt -inkey pub.pem -in plain.txt -out cipher.txt
* openssl pkeyutl -encrypt -inkey pub.pem -in plain.txt -pubout -out cipher.txt
* nessuna delle altre tre scelte

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

Alla luce delle conoscenze attuali:

* Fattorizzare n e rompere RSA sono due problemi non correlati tra loro
* Se si trovasse un algoritmo efficiente per rompere RSA allora lo si potrebbe usare per fattorizzare efficientemente n
* Se si trovasse un algoritmo efficiente per fattorizzare n allora lo si potrebbe usare per rompere RSA
* Fattorizzare n è equivalente computazionalmente a rompere RSA

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

* L’architettura del processo di Enrollment realizza un flusso di esecuzione di tipo iterativo
* L’Enrollment prevede una fase di signal processing
* L’Enrollment prevede una fase di feature extraction
* Nessuna delle altre tre scelte

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

* OpenSSL di default utilizza come seme i random bit forniti da /dev/random
* La generazione di bit pseudocasuali di OpenSSL avviene mediante un Probabilistic Random Bit Generator (PRBG)
* Nessuna delle altre tre scelte
* Per la generazione di bit pseudocasuali OpenSSL utilizza di default un OFB DRBG basato su AES a 128 bit

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

* Nessuna delle altre tre scelte
* È possibile effettuare il “resume” di una sessione in base al valore del campo client\_version
* È possibile effettuare il “resume” di una sessione anche se Client e Server non hanno memorizzato i parametri di sessione
* È possibile effettuare il “resume” di una sessione mediante il Change Cipher Spec Protocol

1. Indicare quale tra i seguenti comandi non consente di codificare un messaggio mediante caratteri stampabili. È possibile effettuare una sola scelta:

* Nessuna delle altre tre scelte
* Openssl enc -base64 -in FileInChiaro -out FileCifrato
* Openssl enc -aes-256-cbc -in FileInChiaro -out FileCifrato -e -base64 -pass pass:P1pp0B4ud0
* Openssl enc -aes-256-cbc -in FileInChiaro -out Base64 -e

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

* Nessuna delle altre tre scelte
* In un certificato self-signed il valore del campo Issuer coincide col valore del campo Subject
* In un certificato self-signed il valore del campo Issuer è diverso dal valore del campo Subject
* In un certificato self-signed il valore del campo Issuer coincide col valore del campo Subject della CA che lo ha emesso

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

* SSL/TLS consentono di rinegoziare i parametri SSL/TLS senza interromper la connessione
* SSL/TLS consentono di mantenere una sessione attiva dopo aver chiuso una connessione
* La sessione deve appartenere allo stesso processo che l’ha creata
* Nessuna delle altre tre scelte

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

La modalità operativa Chipher Feedback(CFB) può essere descritta come

* C\_i = M\_i XOR E\_(k XOR i)(C\_{i-1}), con C\_0=IV
* C\_i = C\_{i-1} XOR E\_k (M\_i), con C\_0=IV
* C\_i = M\_i XOR E\_k (C\_{i-1}), con C\_0=IV
* C\_i = M\_i XOR E\_k (M\_i XOR C\_{i-1}), con C\_0=IV

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

* Ogni S-box del DES è una funzione lineare definita tramite un polinomio
* Le altre tre scelte sono tutte sbagliate
* Ogni S-box del DES è una funzione lineare, facile da calcolare e difficile da invertire
* Nessuna S-box del DES è una funzione lineare dell’input

1. Indicare quale tra i seguenti comandi non consente ad Alice di generare una coppia di chiavi RSA con esponente pubblico uguale a 65537. È possibile effettuare una sola scelta

* Openssl genrsa -out -rsaprivatekey.pem -passout pass:P1pp0B4ud0 -aes128 1024 -F4
* Nessuna delle altre tre scelte
* Openssl genrsa -out rsaprivatekey.pem aes 128 1024
* Openssl genrsa -out rsaprivatekey.pem -passout pass:P1pp0B4ud0 -aes128 1024

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

* La firma digitale può essere utilizzata per garantire autenticazione
* La firma digitale può essere utilizzata per garantire confidenzialità
* La firma digitale può essere utilizzata per garantire integrità
* La firma digitale può essere utilizzata per garantire non ripudio

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

* Due certificati rilasciati dalla stessa CA hanno lo stesso campo Issuer Name
* Due certificati rilasciati dalla stessa CA devono sempre avere due numeri di serie differenti
* Due certificati rilasciati dalla stessa CA possono avere campi CN (Common Name) diversi
* Nessuna delle altre tre scelte

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

* Il processo di Autenticazione/Identificazione prevede una fase di digitalizzazione
* Il processo di Autenticazione/Identificazione si occupa di acquisire ed elaborare i dati biometrici degli utenti per prendere una decisione basata sul risultato di un matching tra il template memorizzato e quello corrente
* Il Processo di Autenticazione/Identificazione prevede una fase di matching
* Nessuna delle altre tre scelte

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

* Il Change Cipher Spec Protocol è utilizzato dalle parti per aggiornare la ciphersuite in uso
* Il Change Cipher Spec Protocol è eseguito dalle parti alla cifratura di ogni messaggio
* Il Change Cipher Spec Protocol è caratterizzato dallo scambio di tre messaggi
* Il Change Cipher Spec Protocol è utilizzato dalle parti per aggiornare la versione di TLS in uso

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

* L’analisi dinamica white box richiede la conoscenza di dettagli sulle caratteristiche e sul codice del malware in esame
* L’analisi dinamica white box rappresenta un approccio meno dispendioso rispetto a quello black box
* L’analisi dinamica white box può essere usata in alternativa all’analisi statica
* L’analisi dinamica white box non può essere usata per ottenere informazioni dettagliate

1. Indicare il comando che consente di generare una stringa pseudocasuale stampabile avente lunghezza multipla di 7. È possibile effettuare una sola scelta

* Openssl rand -base64 14 | cut -c1-14
* Openssl rand -base64 32
* Openssl rand -base64 7
* Openssl rand -base64 49

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

* L’AES con chiave di 128 bit ha una sicurezza poco più del doppio del cifrario DES
* L’AES con una chiave di lunghezza 128 bit potrebbe essere rotto nella pratica in pochi giorni da una macchina altamente parallela. Se la chiave fosse di 256 bit, tale attacco richiederebbe qualche anno
* L’AES è un cifrario a blocchi, con una chiave di lunghezza 128, 192 oppure 256 bit. Se la chiave fosse di 128 bit potrebbe essere rotto nella pratica in pochi giorni da una macchina parallela. Tale attacco non è possibile se la chiave fosse di 256 bit
* Tutte le altre risposte sono errate

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

* Se al comando dgst sono passati in input n file, esso calcola la concatenazione degli hash di tali file
* Se al comando dgst sono passati in input n file, esso calcola l’AND degli hash di tali file
* Se al comando dgst sono passati in input n file, esso calcola un hash separato per ciascun file
* Se al comando dgst sono passati in input n file, esso calcola l’hash della concatenazione di tali file

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

* Nessuna delle altre tre scelte
* Base64 consente di memorizzare e trasferire flussi arbitrari di bit mediante caratteri stampabili
* Base64 consente di codificare dati di dimensione arbitraria
* Base64 processa i dati in blocchi da 24 bit e la codifica avviene su blocchi da 6 bit

1. Si assuma che priv.pem sia memorizzata una coppia di chiavi RSA. Indicare il comando per estrarre la chiave pubblica a partire da priv.pem. è possibile effettuare una sola scelta

* Openssl pkeyutl -in priv.pem -out pub.pem
* Openssl rsa -pubin -in priv.pem -pubout -out pub.pem
* Nessuna delle altre tre scelte
* Openssl rsa -in priv.pem -pubout -out pub.pem

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

* Le altre tre scelte sono tutte sbagliate
* Ogni S-box del DES è una permutazione facile da calcolare e difficile da invertire
* Ogni S-box del DES sono definiti come una funzione lineare in un campo finito
* Alcuni S-box del DES possono essere rappresentati da una combinazione lineare del bit in input

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

Secondo le raccomandazioni del NIST, la lunghezza del modulo per lo scambio Diffie-Hellman ad oggi

* Deve essere almeno 4096 bit
* Può essere 256 bit
* Può essere 1024 bit
* Deve essere almeno 2048 bit

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

* Il campo di session\_id del messaggio ClientHello consente al Client di proporre al Server il resume di una sessione precedentemente creata
* Nessuna delle altre tre scelte
* Il campo session\_id del messaggio ClientHello consente al Client di proporre al Server la creazione di una nuova sessione
* Il campo session\_id del messaggio ClientHello consente al Client di comunicare al server l’ID del certificato X.509 da usare per proteggere la sessione

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

* Durante la fase di quiescenza il codice malevolo per attivarsi attente che si verifichi una determinata condizione
* Durante la fase di quiescienza il codice malevolo è più vulnerabile ad eventuali controlli anti-malware
* Durante la fase di quiescienza il codice malevolo è memorizzato all’interno del sistema ma non è attivo
* Durante la fase di quiescienza il codice malevolo è meno vulnerabile ad eventuali controlli anti-malware

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

Secondo le raccomandazioni di NIST, la lunghezza del modulo RSA ad oggi

* Deve essere di almeno 2048 bit
* Deve essere almeno 4096 bit
* Può essere 1024 bit
* Può essere 256 bit

1. Siano priv.pem ed pub.pem una coppia di chiavi RSA, dove priv.pem rappresenta la chiave privata e pub.pem quella pubblica. Indicare il comando che consente di calcolare una firma RSA (firm.txt) per l’hash SHA-384 del file plain.txt. è possibile effettuare una sola scelta

* Openssl sha384 -sign priv.pem -pubout -out firma.txt plain.txt
* Openssl sha384 -sign -pbin priv.pem -out firma.txt plain.txt
* Openssl sha384 -sign priv.pem -out firma.txt plain.txt
* Nessuna delle altre tre scelte

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

il miglior algoritmo conosciuto per fattorizzare un intero n è in media

* Sub-esponenziale nella lunghezza di n
* Polinomiale nella lunghezza di n
* Esponenziale in n
* Esponenziale nella lunghezza di n

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

il miglior algortimo conosciuto per calcolare il logaritmo discreto modulo p è

* Esponenziale nella lunghezza di p
* Sub-esponenziale nella lunghezza di p
* Esponenziale in p
* Polinomiale nella lunghezza di p

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

* Il messaggio Certificate da parte del Server verso il Client è utilizzato per richiedere il Certificato del Client
* Il messaggio certificate è utilizzato per inviare al Client il certificato del Server
* L’invio del messaggio Certificate e ServerKeyExchange da parte del Server verso il Client è mutuamente esclusivo
* Nessuna delle altre tre scelte

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

La modalità operativa Counter (CTR) può essere descritta come

* C\_i = M\_i XOR E\_{k+i}[Counter + i]
* C\_i = M\_i XOR E\_k[Counter XOR i]
* C\_i = M\_i XOR E\_{k XOR i}[Counter + i]
* C\_i = M\_i XOR E\_k[Counter + i]

1. Sia dh.pem il file con i parametri pubblici Diffie-Hellman e siano privA.pem la chiave privata dell’Utente1 e pubB.pem la chiave pubblica dell’Utente2, rispettivamente. Indicare il comando che consente all’Utente1 di ottenere il segreto condiviso, a partire dalle informazioni ricevute dall’Utente2. È possibile effettuare una sola scelta

* Openssl pkeyutl -derive -inkey dh.pem -peerkey pubB.pem -out key.bin
* Openssl pkeyutl -derive -inkey pubB.pem -peerkey privA.pem -out key.bin
* Nessuna delle altre tre scelte
* Openssl pkeyutl -derive -inkey privA.pem -peerkey pubB.pem -out key.bin