Id Lezione 1: Introduzione alle Reti di calcolatori

1. Una Rete di calcolatori è:

A. L'insieme di servizi quali navigazione nel Word Wide Web, posta elettronica, videoconferenze, ecc., disponibili per tutti o per una parte selezionata di utenti

B. Un insieme di dispositivi Hardware collegati l'uno con l'altro da appositi canali di comunicazione, che mediante opportuni Software permettono agli utenti lo scambio di informazioni e la condivisione di risorse e di servizi

C. Un sistema Software complesso che permette agli utenti lo scambio di informazioni e la condivisione di risorse e servizi

D. Il WWW (Word Wide Web)

Answer: B
Section: Reti di calcolatori e Internet

2. Internet è:

A. Un insieme di servizi quali navigazione nel Word Wide Web, posta elettronica, videoconferenze, ecc., disponibili per tutti o per una parte selezionata di utenti

B. Un sistema Software complesso che permette agli utenti lo scambio di informazioni e la condivisione di risorse e servizi

C. L'insieme degli ISP che permettono agli utenti lo scambio di informazioni e la condivisione di risorse e servizi

D. Una specifica rete pubblica che interconnette miliardi di dispositivi distribuiti in tutto il mondo offrendo all'utente una vasta serie di servizi

Answer: D
Section: Reti di calcolatori e Internet

3. Il vantaggio dell'uso dei sistemi di calcolo distribuito che impiegano calcolatori in rete, rispetto ai computer di grandi dimensionei, è dato da:

A. La tolleranza dei guasti, l'economicità dell'Hardware e del Software, la scalabilità che consente gradualità della crescita e flessibilità

B. La possibilità per i programmatori di comunicare tra loro attraverso la rete

C. La possibilità di risolvere un maggior numero di problemi

D. La possibilità di gestire dati di dimensione maggiore

Answer: A
Section: Reti di calcolatori e Internet

4. In una Rete di calcolatori i sistemi periferici, detti anche host, sono:

A. Solo i computer e gli smartphone collegati in rete con l'esclusione di altre tipologie come sensori, elettrodomestici, smart TV, ecc.

B. Tutti i dispositivi collegati in rete con l'esclusione degli smartphone

C. Tutti i dispositivi collegati in rete di qualunque tipologia

D. Solo gli smartphone collegati in rete

Answer: C
Section: Componenti di base di Internet

5. Un router è:

A. Un commutatore di pacchetto usato nelle reti di accesso

B. Un host che scambia messaggi suddivisi in pacchetti con un dispositivo remoto connesso in rete

C. Un sistema periferico che scambia messaggi suddivisi in pacchetti con un dispositivo nel nucleo della rete

D. Un commutatore di pacchetto usato nel nucleo della rete

Answer: D
Section: Componenti di base di Internet

6. Un commutatore a livello di collegamento (link-layer switch) è:
A. Un sistema periferico che scambia messaggi suddivisi in pacchetti con un dispositivo nel nucleo della rete
B. Un host che scambia messaggi suddivisi in pacchetti con un dispositivo remoto connesso in rete
C. Un commutatore di pacchetto usato nelle reti di accesso
D. Un commutatore di pacchetto usato nel nucleo della rete

Answer: C
Section: Componenti di base di Internet

7. La velocità di trasmissione di un collegamento in una rete di calcolatori è misurata in:
A. Numero totale di bit trasmessi
B. Tempo impiegato dall'invio alla ricezione del messaggio
C. Numero di bit al secondo
D. Numero totale di pacchetti trasmessi

Answer: C
Section: Componenti di base di Internet

8. La denominazione ISP (Internet Service Provider) indica:
A. Un insieme di collegamenti e di commutatori di pacchetto gestito da una struttura commerciale o da un ente, che fornisce vari tipi di accesso a Internet tra cui quello residenziale a banda larga, senza fili (wireless) e in mobilità.
B. Il software che consente di pubblicare i siti Web in Internet.
C. Il modem che consente vari tipi di accesso a Internet tra cui quello senza fili (wireless)
D. L'insieme dei router in Internet che collegano le abitazioni degli utenti

Answer: A
Section: Internet Service Provider e protocolli

9. La denominazione Request For Comment indicata dalla sigla RFC è riferita a:
A. Il formato standard dei commenti inseriti nella progettazione delle pagine Web
B. Gli standard per Internet sviluppati dalla Internet Engineering Task Force (IETF)
C. Il formato standard dei commenti inseriti nel Software che gestisce la trasmissione a commutazione di pacchetto
D. Il formato standard dei commenti inseriti nel progetto Hardware di una rete di calcolatori

Answer: B
Section: Internet Service Provider e protocolli

10. Le regole che governano la comunicazione in Internet tra due o più entità remote sono stabilite da:
A. Un programma Software in esecuzione sui sistemi periferici che sono in comunicazione
B. L'invio di messaggi da parte dell'Internet Service Provider (ISP) per gestire il traffico delle trasmissioni
C. Protocolli standard specifici per le varie operazioni da svolgere
D. Una parte dell'Hardware installato sui sistemi periferici che sono in comunicazione

Answer: C
Section: Internet Service Provider e protocolli

DO NOT PAY FOR THIS DOCUMENT - FREE DOCUMENT - NO DOCSITY - NON PAGARE PER QUESTO DOCUMENTO

Id Lezione 2: Accesso a Internet

1. Una rete di accesso:

A. Connette fisicamente un sistema periferico al suo edge router (router di bordo) che è il primo router sul percorso che parte dal sistema di origine verso un qualsiasi altro sistema di destinazione collocato al di fuori della stessa rete di accesso

B. Connette fisicamente il nucleo della rete all'edge router (router di bordo) che è il primo router sul percorso che parte dal sistema di origine verso un qualsiasi altro sistema di destinazione

C. Connette un sistema periferico ad un server mediante una password di autenticazione

D. Connette un sistema periferico al servizio di posta elettronica

Answer: A
Section: Accesso tramite DSL e FTTH

2. Un accesso residenziale ad Internet di tipo DSL (Digital Subscriber Line) utilizza:

A. La rete in fibra ottica fino all'abitazione dell'utente per trasmettere dati digitali convertiti in segnali ottici mediante un terminale ottico detto ONT (Optical Network Terminator)

B. La rete della televisione via cavo per trasmettere dati digitali convertiti mediante un cable modem

C. La rete satellitare della telefonia cellulare

D. La rete analogica telefonica per trasmettere dati digitali convertiti in formato analogico mediante un modem

Answer: D
Section: Accesso tramite DSL e FTTH

3. Un accesso residenziale ad Internet di tipo FTTH (Fiber To The Home) utilizza:

A. La rete analogica telefonica per trasmettere dati digitali convertiti in formato analogico mediante un modem

B. La rete in fibra ottica fino all'abitazione dell'utente per trasmettere dati digitali convertiti in segnali ottici mediante un terminale ottico detto ONT (Optical Network Terminator)

C. La rete della televisione via cavo per trasmettere dati digitali convertiti mediante un cable modem

D. La rete satellitare della telefonia cellulare

Answer: B
Section: Accesso tramite DSL e FTTH

4. In una rete di accesso a Internet DSL lo splitter che si trova nell'abitazione dell'utente effettua:

A. Il collegamento diretto tra il sistema periferico e l'edge router

B. La conversione del segnale analogico proveniente dalla rete telefonica nel formato digitale e lo invia ai sistemi periferici

C. La suddivisione del segnale proveniente dalla linea telefonica esterna all'abitazione, separando il segnale analogico del traffico vocale dal segnale analogico del traffico dati, e invia questi segnali all'apparecchio telefonico ed al modem mediante collegamenti separati

D. Il collegamento diretto tra il sistema periferico e il server del provider che gestisce la connessione

Answer: C
Section: Accesso tramite DSL e FTTH

5. In una rete di accesso a Internet DSL la linea telefonica in uscita dall'abitazione collega lo splitter:

A. Al router del provider che gestisce la connessione

B. Al server del provider che gestisce la connessione

C. Al dispositivo detto OLT (Optica Line Terminator) che si trova nella centrale locale della compagnia telefonica

D. Al dispositivo detto DSLAM (Digital Subscriber Line Access Multiplexer) che si trova nella centrale locale della

compagnia telefonica

Answer: D
Section: Accesso tramite DSL e FTTH

6. In una rete di accesso a Internet DSL il DSLAM (Digital Subscriber Line Access Multiplexer) che si trova nella centrale locale della compagnia telefonica effettua:
A. Il multiplexing raccogliendo i dati provenienti dalle abitazioni e istadandoli su un unico collegamento verso l'ONT (Optical Network Terminator) che costituisce l'edge router del collegamento alla rete
B. Il multiplexing del segnale proveniente dalla linea telefonica esterna all'abitazione, separando il segnale analogico del traffico vocale dal segnale analogico del traffico dati, e invia questi segnali all'apparecchio telefonico ed al modem mediante collegamenti separati
C. Il multiplexing del segnale proveniente dalla linea telefonica esterna all'abitazione, separando il segnale analogico del traffico vocale dal segnale analogico del traffico dati, e invia i dati all'ONT (Optical Network Terminator) che fornisce la conversione tra segnali ottici e segnali elettrici digitali
D. Il multiplexing raccogliendo i dati provenienti dalle abitazioni e istadandoli su un unico collegamento verso il router dell'operatore telefonico, la conversione dei dati da analogico a digitale e la divisioni dei segnali vocali e dei dati digitali istradandoli verso le rispettive reti.

Answer: D
Section: Accesso tramite DSL e FTTH

7. In una rete di accesso a Internet FTTH il dispositivo ONT (Optical Network Terminator) effettua:
A. La conversione tra segnali ottici e segnali elettrici digitali nella centrale locale della compania telefonica e consente il collegamento ad Internet tramite un router del provider
B. Il collegamento finale tra il sistema periferico e l'edge router
C. La conversione tra segnali ottici e segnali elettrici digitali nell'abitazione dell'utente
D. Il collegamento finale tra il sistema periferico e il server del provider che gestisce la connessione

Answer: C
Section: Accesso tramite DSL e FTTH

8. In una rete di accesso a Internet FTTH il dispositivo OLT (Optical Line Terminator) effettua:
A. La conversione tra segnali ottici e segnali elettrici digitali nella centrale locale della compania telefonica e consente il collegamento ad Internet tramite un router del provider
B. La conversione tra segnali ottici e segnali elettrici digitali nell'abitazione dell'utente
C. Il collegamento finale tra il sistema periferico e l'edge router
D. Il collegamento finale tra il sistema periferico e il server del provider che gestisce la connessione

Answer: A
Section: Accesso tramite DSL e FTTH

9. Nell'accesso a Internet mediante una LAN i dispositivi periferici sono collegati:
A. Mediante linee costituite da un doppino di rame intrecciato ad un DSLAM (Digital Subscriber Line Access Multiplexer) che è connesso a Internet tramite un router aziendale
B. Mediante linee costituite da un doppino di rame intrecciato ad un ONT (Optical Network Terminator) che è connesso a Internet tramite un router aziendale
C. Mediante linee costituite da un doppino di rame intrecciato ad uno switch Eternet che è connesso a Internet tramite un router aziendale
D. Mediante linee costituite da un doppino di rame intrecciato ad un OLT (Optical Line Terminator) che è connesso a Internet tramite un router aziendale

Answer: C
Section: Accesso tramite LAN, WLAN e rete satellitare

10. Il simbolo della tecnologia Wi-Fi utilizzata nelle reti WLAN:
A. Indica che il dispositivo è di tipo wireless
B. Indica che il dispositivo consente un collegamento satellitare
C. Rappresenta la certificazione rilasciata dal provider che garantisce la possibilità di connettere il dispositivo wireless ad una rete in fibra ottica basata sullo standard IEEE 802.11
D. Rappresenta la certificazione rilasciata dalla Wi-Fi Alliance che garantisce la interoperabilità dei dispositivi wireless basati sullo standard IEEE 802.11 prodotti da costruttori di Hardware diversi

Answer: D
Section: Accesso tramite LAN, WLAN e rete satellitare

Id Lezione 3: Trasmissione dei dati in Internet

1. In Internet i sistemi periferici utilizzano la tecnica di trasmissione:
A. FTTH (Fiber To The Home)
B. A commutazione di circuito
C. DSL (Digital Subscriber Line)
D. A commutazione di pacchetto

Answer: D
Section: Trasmissione a commutazione di pacchetto

2. Nella trasmissione in Internet un pacchetto è costituito da:
A. Un bit del messaggio trasmesso ed informazioni aggiuntive che identificano la destinazione del messaggio
B. Una parte della sequenza del messaggio trasmesso
C. Tutto il messaggio trasmesso suddiviso in parti
D. Una parte della sequenza del messaggio trasmesso ed informazioni aggiuntive che identificano la destinazione del messaggio

Answer: D
Section: Trasmissione a commutazione di pacchetto

3. La tecnica store and forward nella trasmissione a commutazione di pacchetto stabilisce che:
A. Il router può iniziare la trasmissione di un pacchetto solo quando ha ricevuto tutti i pacchetti in cui è stato suddiviso il messaggio
B. Il provider autorizza la trasmissione dei pacchetti ricevuti dal router
C. Il router può iniziare la trasmissione di un pacchetto solo quando lo ha completamente ricevuto
D. Il router riceva dalla sorgente la password che consente l'accesso dei pacchetti nella destinazione

Answer: C
Section: Trasmissione store and forward

4. Il buffer di output è:
A. Il dispositivo del router che contiene l'indirizzo della destinazione di un pacchetto che il router sta ricevendo fino a quando non si completa la ricezione
B. Un dispositivo di memoria della sorgente in cui sono memorizzati i bit di un pacchetto che la sorgente sta inviando fino a quando non si completa la ricezione.
C. Un dispositivo di memoria del router in cui memorizza i bit di un pacchetto che sta ricevendo fino a quando non si completa la ricezione, ed in cui i pacchetti già ricevuti sono messi in coda in attesa che il collegamento in uscita del router sia disponibile per la trasmissione
D. Un dispositivo di memoria della destinazione in cui il router memorizza i bit di un pacchetto che sta inviando fino a quando non si completa la ricezione.

Answer: C
Section: Trasmissione store and forward

5. In una trasmissione store and forward il tempo di trasmissione di un pacchetto di L bit dalla sorgente al router su un collegamento con velocità di trasmissione R bps è:
A. L-R secondi
B. 2L/R secondi
C. L/R secondi
D. L-2R secondi

Answer: C
Section: Trasmissione store and forward

6. In una trasmissione store and forward il tempo di trasmissione di un solo pacchetto di L bit da una sorgente ad una destinazione entrambe connesse ad un router da collegamenti con velocità di trasmissione R bps è:
A. L/R secondi
B. 2L/R secondi
C. 2L-R secondi
D. L-R secondi

Answer: B
Section: Trasmissione store and forward

7. In una trasmissione store and forward il tempo di trasmissione di N pacchetti di L bit da una sorgente ad una destinazione entrambe connesse ad un router da collegamenti con velocità di trasmissione R bps è:
A. (N+1)(2L-R) secondi
B. (N+1)2L/R secondi
C. (N+1)L/R secondi
D. (N+1)(L-R) secondi

Answer: C
Section: Trasmissione store and forward

8. In una trasmissione store and forward un pacchetto ricevuto da un router che non può essere trasmesso perché il collegamento in uscita non è disponibile viene:
A. Memorizzato e messo in coda in attesa della trasmissione nel buffer di output del computer che invia il messaggio
B. Memorizzato e messo in coda in attesa della trasmissione nel buffer di output del router
C. Memorizzato e messo in coda in attesa della trasmissione nel buffer di output del provider
D. Memorizzato e messo in coda in attesa della trasmissione in un server del provider

Answer: B
Section: Trasmissione store and forward

9. In una trasmissione store and forward il router individua il collegamento in uscita su cui instradare il pacchetto mediante:
A. Informazioni memorizzate nel computer da cui parte la trasmissione del pacchetto
B. La tabella di inoltro che mette in corrispondenza l'indirizzo IP del pacchetto con i collegamenti di entrata del router
C. Informazioni memorizzate in un server del provider
D. La tabella di inoltro che mette in corrispondenza l'indirizzo IP del pacchetto con i collegamenti di uscita del router

Answer: D
Section: Tabelle di inoltro

10. In una trasmissione store and forward le tabelle di inoltro sono:
A. Costruite automaticamente dal computer da cui parte la trasmissione del pacchetto
B. Memorizzate in un server del provider
C. Memorizzate nel computer da cui parte la trasmissione del pacchetto
D. Costruite automaticamentem dal router sulla base di protocolli di instradamento

Answer: D

Section: Tabelle di inoltro

Id Lezione 4: Ritardi nelle Reti a commutazione di pacchetto

1. In una rete a commutazione di pacchetto il ritardo di nodo è:

A. Il tempo impiegato dal nodo per determinare il canale di trasmissione in uscita in base all'indirizzo di destinazione del pacchetto

B. Il ritardo dell'attesa in coda di un pacchetto memorizzato nel buffer di output quando il canale di trasmissione in uscita è occupato

C. Il ritardo per la determinazione della tabella di inoltro nella trasmissione store and forward relativa al collegamento in uscita dal nodo

D. La somma dei ritardi di elaborazione, accodamento, trasmissione e propagazione relativi al collegamento in uscita dal nodo

Answer: D
Section: Ritardo di nodo e perdita di pacchetto

2. I programmi traceroute forniscono:

A. Tutti i possibili percorsi dalla sorgente alla destinazione con l'elenco degli indirizzi IP dei router attraversati e degli ISP cui appartengono

B. Gli indirizzi IP dei router attraversati nella trasmissione di un pacchetto da una sorgente ad una destinazione con i tempi impiegati dal pacchetto per coprire il percorso di andata e ritorno da ogni router, ripetendo la trasmissione in tre prove.

C. Tutti i possibili percorsi dalla sorgente alla destinazione con i tempi totali per trasmettere un pacchetto dalla sorgente alla destinazione su ogni percorso.

D. I collegamenti in uscita da un router con le relative velocità di trasmissione

Answer: B
Section: Ritardo di nodo e perdita di pacchetto

3. L'overflow del buffer di output di un router determina:

A. L'errore nella determinazione del collegamento di uscita su cui instradare un pacchetto in arrivo

B. L'invio di un messaggio al provider per segnalare la mancanza di memoria disponibile per l'esecuzione delle operazioni previste dai protocolli

C. La perdita dei pacchetti in arrivo al router che non possono essere memorizzati nella coda di attesa della trasmissione su un collegamento in uscita

D. L'errore nella determinazione dell'indirizzo IP del sistema periferico destinazione di un pacchetto in arrivo

Answer: C
Section: Ritardo di nodo e perdita di pacchetto

4. Se i pacchetti in arrivo ad un router per mancanza di spazio non possono essere memorizzati nel buffer di output in attesa di essere trasmessi sul collegamento di uscita occupato in una trasmissione, si ha che:

A. I pacchetti vengono memorizzati su un server messo a disposizione dal provider

B. Il router invia al provider una richiesta di spazio aggiuntivo di memorizzazione

C. Il router indirizza i pacchetti su un diverso collegamento di uscita libero

D. I pacchetti vengono eliminati e si ha una perdita di pacchetti per overflow del buffer di output

Answer: D
Section: Ritardo di nodo e perdita di pacchetto

5. In una rete a commutazione di pacchetto il ritardo di elaborazione è il tempo impiegato dal router per:

A. Calcolare il percorso che richiede il tempo più breve per la trasmissione dal sistema periferico sorgente a quello di

destinazione
B. Esaminare l'intestazione del pacchetto e determinare su quale collegamento di uscita dirigerlo, più altro tempo per il controllo ed eventualmente la correzione degli errori avvenuti nella trasmissione dei bit
C. Leggere tutti i bit contenuti nel pacchetto ed elaborali con un algoritmo di compressione per ottenere un pacchetto di lunghezza minore
D. Calcolare il numero di pacchetti che devono arrivare per completare la trasmissione dati tra il sistema periferico sorgente e quello destinazione.

Answer: B
Section: Ritardi di elaborazione e di accodamento

6. In una rete a commutazione di pacchetto il ritardo di accodamento relativo ad un collegamento in uscita da un router è il tempo che:
A. Il router impiega per gestire la coda dei pacchetti memorizzati nel buffer di output relativi ad una trasmissione dati tra la sorgente e la destinazione
B. Il router aspetta per completare la ricezione di tutti i bit che compongono il pacchetto che vengono memorizzati nel buffer di output
C. Un pacchetto rimane nella coda di attesa memorizzata nel buffer di output, prima di essere inviato sul collegamento di uscita del router
D. La destinazione aspetta per completare la ricezione di tutti i bit che compongono il pacchetto che vengono memorizzati nel buffer di output

Answer: C
Section: Ritardi di elaborazione e di accodamento

7. Quando il traffico relativo ad un collegamento di uscita da un router, misurato come rapporto tra il numero medio di bit ricevuti e il numero di bit inviati nell'unità di tempo, risulta maggiore di 1 si ha che:
A. Il ritardo medio di accodamento tende all'infinito poiché la lunghezza della coda di pacchetti memorizzati nel buffer di output in attesa di essere inviati cresce continuamente
B. Il ritardo medio di accodamento cresce linearmente poiché la lunghezza della coda di pacchetti memorizzati nel buffer di output in attesa di essere inviati cresce in proporzione al ritardo
C. Il ritardo medio di accodamento è limitato superiormente da un valore finito poiché la lunghezza della coda di pacchetti memorizzati nel buffer di output in attesa di essere inviati è limitata
D. Il ritardo medio di accodamento è costante poiché la lunghezza della coda di pacchetti memorizzati nel buffer di output in attesa di essere inviati è costante

Answer: A
Section: Ritardi di elaborazione e di accodamento

8. Quando il traffico relativo ad un collegamento di uscita da un router, misurato come rapporto tra il numero medio di bit ricevuti e il numero di bit inviati nell'unità di tempo, risulta minore o uguale a 1 si ha che:
A. Il ritardo medio di accodamento è limitato superiormente da un valore finito
B. Il ritardo medio di accodamento cresce linearmente al tendere a 1 del valore del rapporto che misura il traffico
C. Il ritardo medio di accodamento cresce esponenzialmente al tendere a 1 del valore del rapporto che misura il traffico
D. Il ritardo medio di accodamento è costante

Answer: C
Section: Ritardi di elaborazione e di accodamento

9. In una rete a commutazione di pacchetto il ritardo di trasmissione relativo ad un collegamento in uscita di un

router è il tempo:

A. Che il segnale impiega per percorrere il collegamento dato dal valore del rapporto d/v, dove d è la lunghezza in metri del collegamento che il pacchetto in uscita dal router deve percorrere per giungere al nodo successivo della rete, e v è la velocità in metri al secondo con cui viaggia il segnale caratteristica del materiale di cui è fatto il collegamento

B. Impiegato dal router per instradare il pacchetto verso il collegamento, dato dal valore del rapporto L/R, dove L è la lunghezza in bit del pacchetto ed R è la velocità di trasmissione in bit per secondi del collegamento in uscita dal router

C. Impiegato dal router per esaminare l'intestazione del pacchetto e determinare su quale collegamento di uscita dirigerlo, più altro tempo eventuale per il controllo degli errori avvenuti nella trasmissione dei bit

D. Che un pacchetto impiega per raggiungere il sistema periferico di destinazione

Answer: B

Section: Ritardi di trasmissione e di propagazione

10. In una rete a commutazione di pacchetto il ritardo di propagazione relativo ad un collegamento in uscita di un router è il tempo:

A. Impiegato dal router per instradare il pacchetto verso il collegamento, dato dal valore del rapporto L/R, dove L è la lunghezza in bit del pacchetto ed R è la velocità di trasmissione in bit per secondi del collegamento in uscita del router

B. Che un segnale impiega per percorrere il collegamento dato dal valore del rapporto d/v, dove d è la lunghezza in metri del collegamento che il pacchetto in uscita dal router deve percorrere per giungere al nodo successivo della rete, e v è la velocità in metri al secondo con cui viaggia il segnale caratteristica del materiale di cui è fatto il collegamento

C. Impiegato dal router per esaminare l'intestazione del pacchetto e determinare su quale collegamento di uscita dirigerlo, più altro tempo eventuale per il controllo degli errori avvenuti nella trasmissione dei bit

D. Che un pacchetto impiega per raggiungere il sistema periferico di destinazione

Answer: B

Section: Ritardi di trasmissione e di propagazione

Id Lezione 5: Throughput nelle reti di calcolatori

1. In una rete di calcolatori, il throughput medio end-to-end di una trasmissione di dati tra due sistemi periferici è dato da:

A. Throughput medio end-to-end = T/F bps, dove F è il numero di bit trasmessi tra i due sistemi periferici e T il tempo richiesto dalla trasmissione di tutti i bit

B. Throughput medio end-to-end = F/T bps, dove F è il numero di bit trasmessi tra i due sistemi periferici e T il tempo richiesto dalla trasmissione di tutti i bit

C. Throughput medio end-to-end = 2F/T bps, dove F è il numero di bit trasmessi tra i due sistemi periferici e T il tempo richiesto dalla trasmissione di tutti i bit

D. Throughput medio end-to-end = F+T bps, dove F è il numero di bit trasmessi tra i due sistemi periferici e T il tempo richiesto dalla trasmissione di tutti i bit

Answer: B
Section: Throughput medio

2. In una rete di calcolatori, il tempo di una trasmissione di dati tra due sistemi periferici che si ricava dall'espressione del throughput medio end-to-end è dato da:

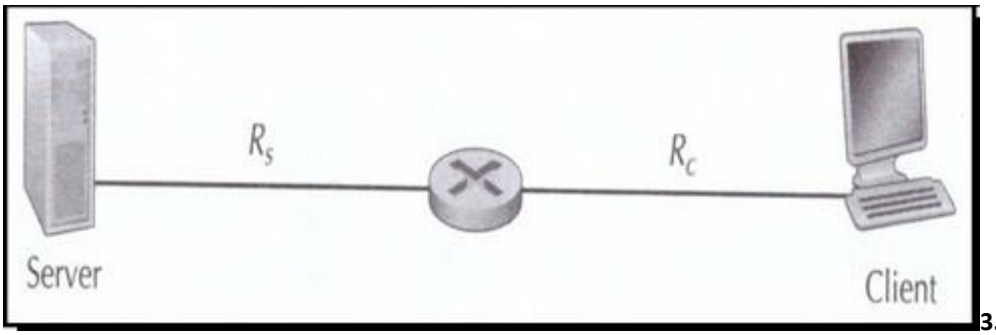
A. Tempo = throughput/F secondi, dove F è il numero di bit trasmessi tra i due sistemi periferici

B. Tempo = F/throughput secondi, dove F è il numero di bit trasmessi tra i due sistemi periferici

C. Tempo = 2F/throughput secondi, dove F è il numero di bit trasmessi tra i due sistemi periferici

D. Tempo = F+throughput secondi, dove F è il numero di bit trasmessi tra i due sistemi periferici

Answer: B
Section: Throughput medio



3. <immagine>

Considerando solo il ritardo di trasmissione nella rete in figura dove Rs bps ed Rc bps sono, rispettivamente, le velocità di trasmissione dei collegamenti server-router e router-client, il throughput medio end-to-end di una trasmissione di dati tra client e server è approssimato da:

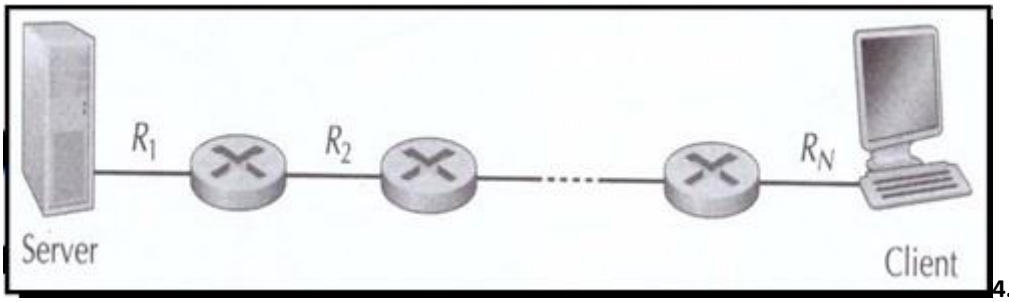
A. Throughput medio end-to-end = (Rs+Rc)/2 bps

B. Throughput medio end-to-end = massimo(Rs, Rc) bps

C. Throughput medio end-to-end = Rs/Rc bps

D. Throughput medio end-to-end = minimo(Rs, Rc) bps

Answer: D
Section: Dipendenza del troughput dalla velocit&ampagrave dei collegamenti

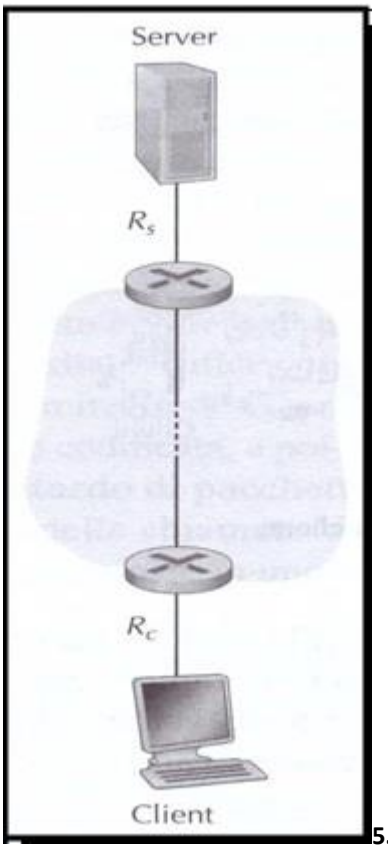


4. <immagine>

Considerando solo il ritardo di trasmissione nella rete in figura dove R₁ bps,…, R_N bps sono le velocità dei collegamenti attraversati nella trasmissione dei dati, il throughput medio end-to-end di una trasmissione di dati tra client e server è approssimato da:

A. Throughput medio end-to-end = massimo(R1,…,RN) bps
B. Throughput medio end-to-end = (R1+…+RN)/N bps
C. Throughput medio end-to-end = minimo(R1, ..., RN) bps
D. Throughput medio end-to-end = R1+…+RN bps

Answer: C
Section: Dipendenza del troughput dalla velocit&ampagrave dei collegamenti



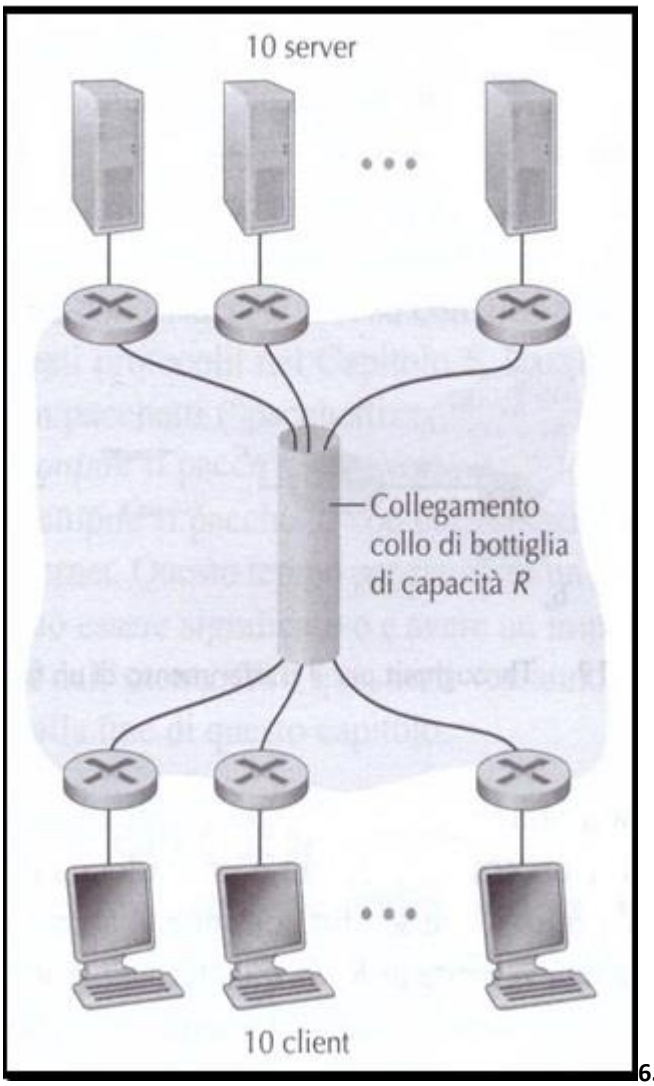
5. <immagine>

Considerando solo il ritardo di trasmissione nella rete in figura dove Rs bps ed Rc bps sono, rispettivamente, le velocità dei collegamenti di accesso al nucleo della rete del server e del client, se tutti i collegamenti presenti nel

nucleo della rete hanno velocità di trasmissione molto alta e molto più grande rispetto alle velocità dei collegamenti di accesso al nucleo della rete del server e del client, il throughput medio end-to-end di una trasmissione di dati tra client e server è approssimato da:

A. Throughput medio end-to-end = (Rs+Rc)/2 bps
B. Throughput medio end-to-end = massimo(Rs,Rc) bps
C. Throughput medio end-to-end = Rs/Rc bps
D. Throughput medio end-to-end = minimo(Rs, Rc) bps

Answer: D
Section: Dipendenza del troughput dalla velocit&ampagrave dei collegamenti



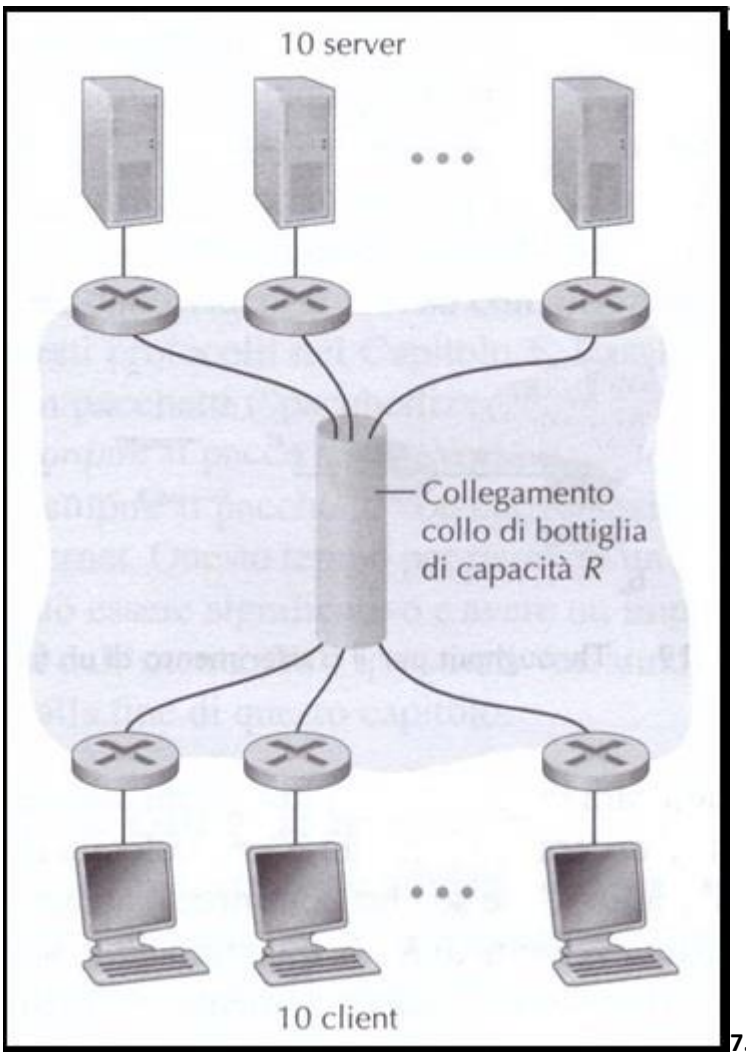
6. <immagine>

Considerando solo il ritardo di trasmissione nella rete in figura, quando attraverso il collegamento comune di velocità R nel nucleo della rete, condiviso ad intervalli di tempo uguali, avvengono 10 trasmissioni di dati contemporane tra 10 coppie client-server, la velocità del collegamento comune disponibile per ogni trasferimento dati tra una coppia client-server è:

A. Il valore R/10 bps
B. Il valore R bps
C. Il valore 10R bps

D. Il valore 10/R bps

Answer: A
Section: Dipendenza del troughput dal traffico nella rete

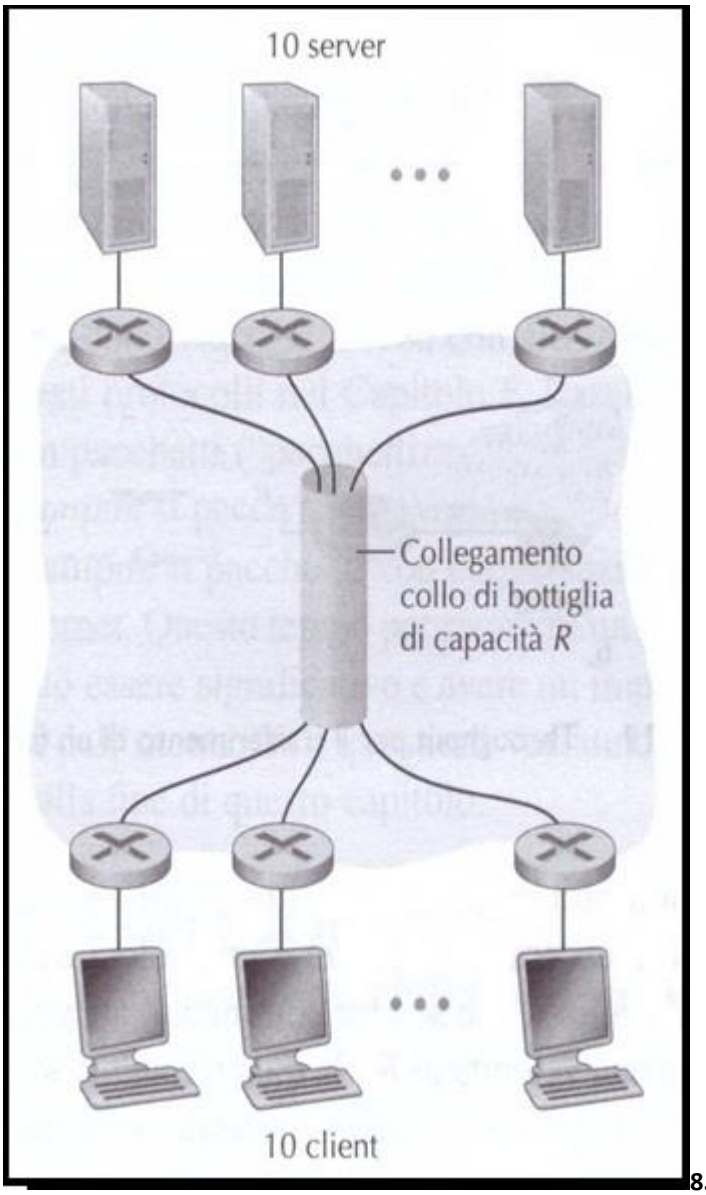


7. <immagine>

Considerando solo il ritardo di trasmissione nella rete in figura, quando attraverso il collegamento comune di velocità R nel nucleo della rete, condiviso ad intervalli di tempo uguali, avvengono 10 trasmissioni di dati contemporane tra 10 coppie client-server, se la velocità del collegamento comune disponibile per ogni trasferimento dati rimane superiore alle velocità di accesso al nucleo della rete Rc dei client ed Rs dei server, il throughput medio end-to-end di una trasmissione di dati tra una coppia client-server è approssimato da:

A. Throughput medio end-to-end = R bps
B. Throughput medio end-to-end = massimo(Rs,Rc) bps
C. Throughput medio end-to-end = minimo(Rs, Rc) bps
D. Throughput medio end-to-end =(Rs+Rc)/2 bps

Answer: C
Section: Dipendenza del troughput dal traffico nella rete



8. <immagine>

Considerando solo il ritardo di trasmissione nella rete in figura, quando attraverso il collegamento comune di velocità R nel nucleo della rete, condiviso ad intervalli di tempo uguali, avvengono 10 trasmissioni di dati contemporane tra 10 coppie client-server, se la velocità del collegamento comune disponibile per ogni trasferimento dati diventa minore delle velocità di accesso al nucleo della rete Rc dei client e Rs dei server, il throughput medio end-to-end di una trasmissione di dati tra una coppia client-server è approssimato da:

A. Throughput medio end-to-end = (Rs+Rc)/2 bps
B. Throughput medio end-to-end = minimo(Rs, Rc) bps
C. Throughput medio end-to-end = velocità ridotta offerta dal collegamento comune
D. Throughput medio end-to-end = massimo(Rs, Rc) bps

Answer: C
Section: Dipendenza del troughput dal traffico nella rete

9. In una rete di calcolatori, il throughput medio end-to-end di una trasmissione di dati tra due sistemi periferici è

una misura:

A. Del numero di errori che si verificano nella trasmissione client-server
B. Delle prestazioni del sistema periferico client
C. Delle prestazioni della rete
D. Delle prestazioni del sistema periferico server

Answer: C
Section: Dipendenza del troughput dal traffico nella rete

10. In una rete di calcolatori, la misura del throughput medio end-to-end di una trasmissione di dati tra due sistemi periferici è espressa in:

A. Bit
B. Bit al secondo
C. Metri al secondo
D. Secondi

Answer: B
Section: Dipendenza del troughput dal traffico nella rete

Id Lezione 6: Internet: una rete di reti

1. La strutturazione di Internet come reti di reti consiste:

A. Nella suddivisione delle reti degli ISP in gruppi corrispondenti a tre livelli di una gerachia dove: gli ISP di accesso che hanno come clienti gli utenti finali costituiscono il livello più basso e pagano il proprio traffico dati agli ISP regionali posti nel livello superiore, che a loro volta sono clienti degli ISP di livello 1, posti nel grado più alto della gerarchia che non pagano per il proprio traffico dati. A questa gerarchia si aggiungono le reti private dei distributori di contenuti, di cui Google è un esempio

B. Nella suddivisione delle reti degli ISP in gruppi corrispondenti a due livelli di una gerachia dove: gli ISP di accesso che hanno come clienti gli utenti finali costituiscono il livello più basso e pagano il proprio traffico dati agli ISP regionali posti nel livello superiore che pagano in funzione del traffico dati che si scambiano tra loro. A questa gerarchia si aggiungono le reti private dei distributori di contenuti, di cui Google è un esempio

C. Nella suddivisione delle reti in due gruppi costituiti dalle reti pubbliche degli ISP di accesso che forniscono traffico agli utenti finali mediante tecnologie di trasmissione di vario tipo (DDL, FTTH, Wi-Fi, satellitare) e dalle reti private che si occupano di distribuire contenuti, di cui Google è un esempio

D. Nella rete costituita dalla connessione tra le sottoreti degli ISP di accesso che forniscono traffico agli utenti finali mediante tecnologie di trasmissione di vario tipo (DDL, FTTH, Wi-Fi, satellitare). A questa rete di reti si aggiungono le reti private dei distributori di contenuti, di cui Google è un esempio

Answer: A
Section: Gerarchia di reti, multi-homing, Point of Presence

2. Il multi-homing consiste:

A. Nella connessione a Internet pagando il traffico ad un ISP regionale che a sua volta paga il traffico ad un fornitore di livello 1

B. Nella possibilità di connettersi affittando un collegamento ad alta velocità ad un gruppo di router che appartengono alla rete di un ISP e sono posizionati fisicamente vicini

C. Nella possibilità per tutti gli ISP di connettersi a due o più fornitori di livello superiore. Sono esclusi gli ISP di livello 1 che non pagano fornitori

D. In un collegamento tra due sistemi periferici che attraversa più ruter appartenenti a reti di ISP di livello gerarchico diverso

Answer: C
Section: Gerarchia di reti, multi-homing, Point of Presence

3. Un PoP (Point of Presence) consiste:

A. Nella possibilità per tutti gli ISP di connettersi a due o più fornitori di livello superiore mediante un collegamento ad alta velocità. Sono esclusi gli ISP di livello 1 che non pagano fornitori

B. In un gruppo di router collocati fisicamente vicini che appartiene alla rete di un ISP fornitore. L'ISP fornitore che possiede un PoP offre ai propri ISP clienti la possibilità di collegare un loro router direttamente ad un router del PoP mediante, un collegamento ad alta velocità. Gli ISP di accesso che hanno come clienti gli utenti finali non posseggono PoP.

C. In un gruppo di router collocati fisicamente vicini che consentono ad ISP di ottimizzare i costi di una connessione di tipo peering tra le loro reti. Gli ISP clienti hanno la possibilità di collegare un loro router direttamente ad un router del PoP mediante un collegamento ad alta velocità.

D. In un insieme di attrezzature e servizi che consentono ad ISP di ottimizzare i costi di una connessione di tipo peering tra le loro reti

Answer: B
Section: Gerarchia di reti, multi-homing, Point of Presence

4. Un servizio di housing (colocation) consiste:

A. Nel collegamento tra due sistemi periferici tramite ruters che appartengono a reti di ISP dello stesso livello gerarchico

B. Nella possibilità per tutti gli ISP di connettersi a due o più fornitori di livello superiore. Sono esclusi gli ISP di livello 1 che non pagano fornitori

C. Nel realizzare una connessione di tipo peering tra due ISP mediante le attrezzature di un ISP di livello gerarchico superiore che garantisce la gestione degli aspetti hardware, software ed infrastrutturali come il condizionamento termico e la vigilanza

D. Nel concedere in affitto uno spazio fisico in un Data center (generalmente all'interno di appositi armadi detti rack) dove posizionare i router di proprietà dell'ISP che fruisce del servizio. Il Data center garantisce la gestione degli aspetti hardware, software ed infrastrutturali come il condizionamento termico e la vigilanza

Answer: D
Section: Gerarchia di reti, multi-homing, Point of Presence

5. La rete di un ISP di livello 1 si connette a Internet:

A. Solo con connessioni ad IXP (Internet exchange Point)
B. Solo con connessione di tipo peering
C. Solo con connessioni ad PoP (Point of Presence)
D. Solo con modalità multi-homing

Answer: B
Section: Peering ed Internet exchange Point

6. Un ISP di accesso si può connettere ad ISP di livello 1:

A. Solo con connessioni ad IXP (Internet exchange Point)
B. Sia pagando il traffico ad un ISP regionale che a sua volta paga il traffico ad un fornitore di livello 1, sia direttamente all'ISP di livello 1 pagando il relativo traffico
C. Solo con connessioni a PoP (Point of Presence)
D. Solo tramite un ISP regionale

Answer: B
Section: Peering ed Internet exchange Point

7. Una connessione di tipo peering tra reti di ISP consiste:

A. Nel pagamento da parte di un ISP del traffico fornito da un fornitore di livello superiore
B. In una connessione attraverso collegamenti ad alta velocità
C. In una connessione in cui nessuno degli ISP collegati paga l'altro per lo scambio di traffico che avviene tra le loro reti, ma ciascuno raccoglie separatamente per se stesso i pagamenti dai propri clienti
D. In una connessione diretta tramite un PoP (Point of Presence) mediante un collegamento ad alta velocità

Answer: C
Section: Peering ed Internet exchange Point

8. Un IXP (Internet exchange Point) consiste:

A. Nel collegamento tra due sistemi periferici tramite un router nella rete di un ISP regionale
B. In un gruppo di router collocati fisicamente vicini che appartiene alla rete di un ISP fornitore. L'ISP fornitore che possiede un IXP offre ai propri ISP clienti la possibilità di collegare un loro router direttamente ad un router del IXP, mediante un collegamento ad alta velocità. Gli ISP di accesso che hanno come clienti gli utenti finali non posseggono IXP.
C. Nel pagamento ad un ISP di livello gerarchico superiore del traffico che passa attraverso un router

D. In un insieme di attrezzature e servizi che consentono ad ISP di ottimizzare i costi di una connessione di tipo peering tra le loro reti

Answer: D
Section: Peering ed Internet exchange Point

9. La gestione di un IXP (Internet exchange Point) è:
A. Affidata agli ISP che gestiscono l'accesso degli utenti finali
B. Affidata agli ISP di livello 1
C. Di tipo commerciale, in cui l'azienda che ha creato e che gestisce l'IXP offre a pagamento i servizi agli ISP che ne diventano clienti, oppure di tipo consortile, in cui gli ISP che intendono stabilire un collegamento di tipo peering si riuniscono in associazioni e partecipano alla gestione dell'IXP
D. Affidata all'ISP a cui appartiene il router che effettua lo smistamento del traffico dati

Answer: C
Section: Peering ed Internet exchange Point

10. Una rete privata di un grande distributore di contenuti come Google può connettersi:
A. Anche alle reti di ISP di livello basso tramite connessioni a PoP (Point of Presence) pagando il traffico dei dati
B. Anche alle reti di ISP di livello basso con collegamenti di tipo peering sia direttamente sia tramite connessioni a IXP (Internet exchange Point)
C. Anche alle reti di ISP di livello basso con modalità multi-homing
D. Anche alle reti di ISP di livello basso tramite un servizio di housing (colocation)

Answer: B
Section: Reti private di distribuzione di contenti

Id Lezione 7: Architettura a livelli: suite di protocolli ISO/OSI e TCP/IP

1. Il vantaggio della modulatità offerto dalla Architettura a livelli consiste nella possibilità di:
A. Cambiare un host periferico senza dover cambiare l'implementazione della parte rimanente del sistema
B. Aggiungere un numero non limitato di dispositivi periferici connessi in rete
C. Scegliere più ISP (Internet Service Provider) per collegarsi alla rete
D. Cambiare l'implementazione dei servizi forniti dal protocollo di un particolare livello senza dover cambiare l'implementazione della parte rimanente del sistema

Answer: D
Section: Architettura a livelli di una rete a commutazione di pacchetto

2. La suite di protocolli ISO/OSI è:
A. Il Modello della pila di protocolli di rete definita da 7 protocolli nello standard del 1984
B. Il Modello della pila di protocolli implementati in Internet definita da 4 livelli nello standard RFC 1122 del 1989
C. Il Modello della pila di protocolli implementati in Internet definita da 4 protocolli nello standard RFC 1122 del 1989
D. Il Modello della pila di protocolli di rete definita da 7 livelli nello standard del 1984

Answer: D
Section: Suite di protocolli ISO/OSI

3. Il livello di Applicazione dello standard ISO/OSI offre servizi:
A. Di crittografia e di compressione del testo
B. Per consentire alle applicazioni di interpretare il significato semantico dei dati
C. Per i processi relativi all'esecuzione delle applicazioni sui sistemi periferici sorgente e destinazione
D. Che consentono la sincronizzazione dello scambio dei dati

Answer: C
Section: Suite di protocolli ISO/OSI

4. Il livello di Trasporto dello standard ISO/OSI offre servizi:
A. Che consentono la comunicazione tra i nodi della rete che vengono attraversati nel percorso che va dal sistema periferico sorgente al sistema periferico destinazione
B. Che permettono un trasferimento di dati affidabile, effettuando anche un controllo degli errori e delle perdite di pacchetti tra due sistemi periferici
C. Per il trasferimento di dati tra nodi adiacenti attraverso il tipo di collegamento che sussiste tra di loro
D. Necessari a livello Hardware per controllare il flusso di dati attraverso i collegamenti e le connessioni ai dispositivi che permettono il passaggio dei segnali che rappresentano le informazioni

Answer: B
Section: Suite di protocolli ISO/OSI

5. Il livello di Rete dello standard ISO/OSI offre servizi:
A. Per il trasferimento di dati tra nodi adiacenti attraverso il tipo di collegamento che sussiste tra di loro
B. Che permettono un trasferimento di dati affidabile, effettuando anche un controllo degli errori e delle perdite di pacchetti tra due sistemi periferici
C. Che consentono la comunicazione tra i nodi della rete che vengono attraversati nel percorso che va dal sistema periferico sorgente al sistema periferico destinazione
D. Necessari a livello Hardware per controllare il flusso di dati attraverso i collegamenti e le connessioni ai dispositivi che permettono il passaggio dei segnali che rappresentano le informazioni

Answer: C
Section: Suite di protocolli ISO/OSI

6. Il livello di Collegamento dello standard ISO/OSI offre servizi:
A. Necessari a livello Hardware per controllare il flusso di dati attraverso i collegamenti e le connessioni ai dispositivi che permettono il passaggio dei segnali che rappresentano le informazioni
B. Per il trasferimento di dati tra nodi adiacenti attraverso il tipo di collegamento che sussiste tra di loro
C. Che permettono un trasferimento di dati affidabile, effettuando anche un controllo degli errori e delle perdite di pacchetti tra due sistemi periferici
D. Che consentono la comunicazione tra i nodi della rete che vengono attraversati nel percorso che va dal sistema periferico sorgente al sistema periferico destinazione

Answer: B
Section: Suite di protocolli ISO/OSI

7. Il livello Fisico dello standard ISO/OSI offre servizi:
A. Che permettono un trasferimento di dati affidabile, effettuando anche un controllo degli errori e delle perdite di pacchetti tra due sistemi periferici
B. Per il trasferimento di dati tra nodi adiacenti attraverso il tipo di collegamento che sussiste tra di loro
C. Necessari a livello Hardware per controllare il flusso di dati attraverso i collegamenti e le connessioni ai dispositivi che permettono il passaggio dei segnali che rappresentano le informazioni
D. Che consentono la comunicazione tra i nodi della rete che vengono attraversati nel percorso che va dal sistema periferico sorgente al sistema periferico destinazione

Answer: C
Section: Suite di protocolli ISO/OSI

8. Rispetto ai modelli ISO/OSI e TCP/IP l'approccio cross-layer è:
A. Diverso perché introduce la capacità di scambiare informazioni anche tra protocolli relativi a livelli diversi
B. Uguale perché i protocolli possono comunicare solo con protocolli dello stesso livello
C. Diverso perché introduce la capacità di scambiare l'ordine gerarchico dei livelli
D. Diverso perché unifica il livello di rete con quello di collegamento

Answer: A
Section: Suite di protocolli ISO/OSI

9. La suite di protocolli TCP/IP è:
A. Il Modello della pila di protocolli implementati in Internet definita da 4 protocolli nello standard RFC 1122 del 1989
B. Il Modello della pila di protocolli implementati in Internet definita da 4 livelli nello standard RFC 1122 del 1989
C. Il Modello della pila di protocolli di rete definita da 7 protocolli nello standard del 1984
D. Il Modello della pila di protocolli di rete definita da 7 livelli nello standard del 1984

Answer: B
Section: Suite di protocolli Internet (TCP/IP)

10. I modelli di protocolli ISO/OSI e TCP/IP sono:
A. Diversi perché i livelli di Presentazione e di Sessione non sono presenti nello standard ISO/OSI
B. Diversi perché i livelli di Presentazione e di Sessione non sono presenti nello standard TCP/IP
C. Diversi per l'ordine gerarchico dei livelli dei protocoli
D. Denominazioni differenti di una stessa suite di protocolli di Internet

Answer: B
Section: Suite di protocolli Internet (TCP/IP)

Id Lezione 8: Incapsulamento nella suite dei protocolli Internet

1. La denominazione dei pacchetti relativi ai livelli del Modello TCP/IP è:

A. Messaggio per il livello di applicazione, datagramma per il livello di trasporto, segmento per il livello di rete, frame per il livello di collegamento, il singolo bit per il livello fisico

B. Messaggio per il livello di applicazione, segmento per il livello di trasporto, frame per il livello di rete, datagramma per il livello di collegamento, il singolo bit per il livello fisico

C. Messaggio per il livello di applicazione, segmento per il livello di trasporto, datagramma per il livello di rete, frame per il livello di collegamento, il singolo bit per il livello fisico

D. Messaggio per il livello di applicazione, frame per il livello di trasporto, segmento per il livello di rete, datagramma per il livello di collegamento, il singolo bit per il livello fisico

Answer: C

Section: I pacchetti nella suite dei protocolli Internet (TCP/IP)

2. I principali protocolli del livello di applicazione del Modello TCP/IP sono:

A. Il protocollo TCP che garantisce una trasmissione affidabile tra mittente e destinatario con ritrasmissione dei pacchetti persi, il protocollo UDP che fornisce una trasmissione con possibilità di perdita di pacchetti ma più veloce

B. Il protocollo IP che gestisce l'instradamento dei pacchetti consentendo di interconnettere reti eterogenee per tecnologia, prestazioni e gestione

C. Il protocollo HTTP per il trasferimento di documenti Web, il protocollo SMTP per la posta elettronica, il protocollo FTP per il trasferimento di file tra sistemi remoti, il protocollo DNS per la conversione di indirizzi simbolici in indirizzi numerici IP

D. Il protocollo Ethernet che gestisce le trasmissioni nelle LAN

Answer: C

Section: I pacchetti nella suite dei protocolli Internet (TCP/IP)

3. I principali protocolli del livello di trasferimento del Modello TCP/IP sono:

A. Il protocollo HTTP per il trasferimento di documenti Web, il protocollo SMTP per la posta elettronica, il protocollo FTP per il trasferimento di file tra sistemi remoti, il protocollo DNS per la conversione di indirizzi simbolici in indirizzi numerici IP

B. Il protocollo Ethernet che gestisce le trasmissioni nelle LAN

C. Il protocollo IP che gestisce l'instradamento dei pacchetti consentendo di interconnettere reti eterogenee per tecnologia, prestazioni e gestione

D. Il protocollo TCP che garantisce una trasmissione affidabile tra mittente e destinatario con ritrasmissione dei pacchetti persi, il protocollo UDP che fornisce una trasmissione con possibilità di perdita di pacchetti ma più veloce

Answer: D

Section: I pacchetti nella suite dei protocolli Internet (TCP/IP)

4. Il principale protocollo del livello di rete del Modello TCP/IP è:

A. Il protocollo Ethernet che gestisce le trasmissioni nelle LAN

B. Il protocollo HTTP per il trasferimento di documenti Web, il protocollo SMTP per la posta elettronica, il protocollo FTP per il trasferimento di file tra sistemi remoti, il protocollo DNS per la conversione di indirizzi simbolici in indirizzi numerici IP

C. Il protocollo TCP che garantisce una trasmissione affidabile tra mittente e destinatario con ritrasmissione dei pacchetti persi, il protocollo UDP che fornisce una trasmissione con possibilità di perdita di pacchetti ma più veloce

D. Il protocollo IP che gestisce l'instradamento dei pacchetti consentendo di interconnettere reti eterogenee per tecnologia, prestazioni e gestione

Answer: D
Section: I pacchetti nella suite dei protocolli Internet (TCP/IP)

5. Il campo payload di un pacchetto gestito al livello di Trasporto è costituito da:
A. Un Datagramma fornito dal livello di Rete
B. Un Segmento fornito dal livello di Trasporto
C. Un Messaggio fornito dal livello di Applicazione
D. Un Frame fornito dal livello di Collegamento

Answer: C
Section: Incapsulamento

6. Il campo payload di un pacchetto gestito al livello di Rete è costituito da:
A. Un Segmento fornito dal livello di Trasporto
B. Un Messaggio fornito dal livello di Applicazione
C. Un Datagramma fornito dal livello di Rete
D. Un Frame fornito dal livello di Collegamento

Answer: A
Section: Incapsulamento

7. Il campo payload di un pacchetto gestito al livello di Collegamento è costituito da:
A. Un Segmento fornito dal livello di Trasporto
B. Un Frame fornito dal livello di Collegamento
C. Un Messaggio fornito dal livello di Applicazione
D. Un Datagramma fornito dal livello di Rete

Answer: D
Section: Incapsulamento

8. Il campo payload di un pacchetto gestito al livello Fisico è costituito da:
A. Un Segmento fornito dal livello di Trasporto
B. Un Datagramma fornito dal livello di Rete
C. Un Messaggio fornito dal livello di Applicazione
D. Un Frame fornito dal livello di Collegamento

Answer: D
Section: Incapsulamento

9. In una rete a commutazione di pacchetto basata sull'Architettura a livelli l'incapsulamento è:
A. L'operazione che inserisce, nel campo payload di un pacchetto relativo ad un livello, il pacchetto gestito dal livello superiore
B. L'operazione che inserisce, nel campo payload del pacchetto relativo ad un livello, le informazioni aggiuntive gestite dai protocolli di tale livello
C. L'ordinamento nella pila (stack) dei livelli che costituiscono la suite di protocolli dell'Architettura
D. La memorizzazione dei pacchetti nel buffer di output di un router

Answer: A
Section: Incapsulamento

10. In una rete a commutazione di pacchetto basata sull'Architettura a livelli l'header è:

A. Il livello più alto nella gerarchia definita dal Modello standard ISO/OSI
B. Il campo del pacchetto relativo ad un livello, che contiene il pacchetto gestito dal livello superiore
C. Il campo del pacchetto relativo ad un livello, che contiene le informazioni aggiuntive gestite dai protocolli di tale livello
D. Il livello più alto nella gerarchia definita dal Modello standard TCP/IP

Answer: C
Section: Incapsulamento

Id Lezione 9: Sicurezza in Internet

1. Un malware è:

A. Un Software per impedire un attacco sul computer di un utente attraverso una attività svolta in rete

B. Un Software dannoso che l'autore di un attacco può installare sul computer di un utente attraverso una attività svolta in rete

C. Un dispositivo Harware per impedire un attacco sul computer di un utente attraverso una attività svolta in rete

D. Gli strumenti Hardware e Software utilizzati per impedire gli attacchi mediante attività svolte in rete

Answer: B

Section: Malware installati sugli host tramite Internet

2. Un malware viene detto autoreplicante quando:

A. Può diffondere in rete copie di se stesso, che effettuano lo stesso tipo di attacco su altri computer

B. Può diffondere in rete copie dei file memorizzati sul computer infettato di un utente inconsapevole

C. Può copiare sul computer dell'attaccante i i file memorizzati sul computer infettato di un utente inconsapevole

D. Può ripetere un attacco informatico ad intervalli di tempo regolari su uno stesso computer

Answer: A

Section: Malware installati sugli host tramite Internet

3. Si definisce botnet:

A. Un Software che diffonde in rete copie dei file memorizzati su un computer infettato

B. Un attacco informatico che si ripete ad intervalli di tempo regolari su uno stesso computer

C. La rete di computer infettati che l'autore di un attacco controlla

D. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server

Answer: C

Section: Malware installati sugli host tramite Internet

4. Un virus informatico è:

A. Un Software che diffonde in rete copie dei file memorizzati su un computer infettato

B. Un malware autoreplicante che può infettare un dispositivo senza alcuna interazione esplicita con l'utente

C. La rete di computer infettati che l'autore di un attacco controlla

D. Un malware autoreplicante che richiede una qualche forma di interazione con l'utente per poter infettare il dispositivo

Answer: D

Section: Malware installati sugli host tramite Internet

5. Un worm informatico è:

A. Un malware autoreplicante che richiede una qualche forma di interazione con l'utente per poter infettare il dispositivo

B. Un malware autoreplicante che può infettare un dispositivo senza alcuna interazione esplicita con l'utente

C. La rete di computer infettati che l'autore di un attacco controlla

D. Un Software che copia sul computer dell'attaccante i file memorizzati sul computer di un utente inconsapevole

Answer: B

Section: Malware installati sugli host tramite Internet

6. Una DoS provocata da un attacco alla vulnerabilità del sistema è:

A. Una interruzione del servizio causata dall'invio ad una applicazione vulnerabile o al Sistema Operativo in esecuzione sul server sotto attacco, di una sequenza di pacchetti opportunamente costruiti per determinare il blocco del servizio o anche lo spegnimento del server

B. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server

C. Una interruzione del servizio causata da una gran numero di connessioni TCP generate dall'attaccante e mantenute tutte aperte per ingorgare la capacità ricettiva del server

D. La diffusione in rete di copie dei file memorizzati su un computer

Answer: A

Section: Attacchi ai server e all'infrastruttura di rete

7. Una DoS provocata da una inondazione di banda è:

A. Una interruzione del servizio causata dall'invio ad una applicazione vulnerabile o al Sistema Operativo in esecuzione sul server sotto attacco, di una sequenza di pacchetti opportunamente costruiti per determinare il blocco del servizio o anche lo spegnimento del server

B. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server

C. Una interruzione del servizio causata da una gran numero di connessioni TCP generate dall'attaccante e mantenute tutte aperte per ingorgare la capacità ricettiva del server

D. La diffusione in rete di copie dei file memorizzati su un computer

Answer: B

Section: Attacchi ai server e all'infrastruttura di rete

8. Una DoS provocata da una inondazione di connessione è:

A. Una interruzione del servizio causata da una gran numero di connessioni TCP generate dall'attaccante e mantenute tutte aperte per ingorgare la capacità ricettiva del server

B. Una interruzione del servizio causata dall'invio di una sequenza di pacchetti opportunamente costruiti ad una applicazione vulnerabile o al Sistema Operativo in esecuzione sul server sotto attacco, in grado di determinare il blocco del servizio o anche lo spegnimento del server

C. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server

D. La diffusione in rete di copie dei file memorizzati su un computer

Answer: A

Section: Attacchi ai server e all'infrastruttura di rete

9. Il packet sniffing è:

A. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server

B. La diffusione in rete di copie dei file memorizzati su un computer

C. La copia mediante un ricevitore passivo di ogni pacchetto in transito su una connessione all'insaputa degli utenti collegati che non hanno modo per potersene accorgere

D. Un malware autoreplicante che richiede una qualche forma di interazione con l'utente per poter infettare il dispositivo

Answer: C

Section: Packet sniffing e Internet delle cose

10. La difesa da una attività di packet sniffing è costituita:

A. Dalla installazione di opportuni dispositivi Hardware

B. Dall'uso di tecniche di crittografia per codificare i messaggi trasmessi

C. Dal controlo del numero di accessi alla rete effettuati dal computer

D. Dal settaggio di opportuni paramentri di trasmissione dei messaggi nel sistema periferico sorgente

Answer: B

Section: Packet sniffing e Internet delle cose

Id Lezione 10: Concetti base di sicurezza

1. L'insieme delle misure adottate per proteggere i dati durante la loro trasmissione attraverso una serie di reti interconnesse:
A. Computer Security
B. Network Security
C. Internet Security
D. Access Security

Answer: C
Section: Sicurezza delle informazioni

2. Quali aspetti non sono da considerare fondamentali nella progettazione di un sistema di sicurezza:
A. Gestione delle informazioni segrete
B. Analisi dei potenziali attacchi
C. Praticabilità
D. Posizione fisica del server

Answer: D
Section: Sicurezza delle informazioni

3. Un attacco alla sicurezza è:
A. Qualsiasi azione che compromette la sicurezza delle informazioni
B. Processo progettato per rilevare, prevenire o riparare i danni prodotti da un attacco alla sicurezza
C. Servizio che migliora la sicurezza dei sistemi di elaborazione e trasmissione
D. La cancellazione di informazioni

Answer: A
Section: Lâ€™architettura di sicurezza del modello OSI

4. Una minaccia è:
A. Un potenziale pericolo
B. Un attacco
C. Un tipo di attacco
D. Una violazione

Answer: A
Section: Lâ€™architettura di sicurezza del modello OSI

5. Un attacco passivo tenta di:
A. Modificare le informazioni
B. Rilevare o utilizzare le informazioni del sistema ma non agisce sulle sue risorse
C. Alterare il funzionamento di un sistema
D. Inibire il funzionamento di un sistema

Answer: B
Section: Lâ€™architettura di sicurezza del modello OSI

6. Quando un sistema è sottoposto ad un attacco passivo:
A. Il destinatario dei messaggi non riceve niente
B. Il mittente dei messaggi capisce che la trasmissione non va a buon fine

C. I messaggi sono inviati e ricevuti in maniera apparentemente normale
D. Il destinatario si accorge che qualcuno sta ascoltando la trasmissione

Answer: C
Section: Attacchi passivi

7. In un attacco passivo di analisi del traffico:
A. Se il traffico è cifrato non ci sono problemi
B. Anche se il traffico è cifrato, l'attaccante riesce lo stesso a leggere il messaggio
C. Il destinatario si accorge dell'attacco
D. L'attaccante riesce ad estrarre informazioni sul tipo di trasmissione

Answer: D
Section: Attacchi passivi

8. Un attacco attivo prevede:
A. La modifica del flusso dei dati o la creazione di un flusso falsificato
B. Necessariamente l'interazione con il mittente del messaggio
C. La precedente realizzazione di un attacco passivo
D. Necessariamente l'accesso ai dati trasmessi

Answer: A
Section: Attacchi attivi

9. Quali di questi attacchi non è attivo:
A. Ripetizione
B. Mascheramento
C. Denial-of-Service
D. Analisi del traffico

Answer: D
Section: Attacchi attivi

10. Un attaccante tenta di accedere all'account di posta di un altro utente, si tratta di un attacco di:
A. Mascheramento
B. Denial-of-Service
C. Intercettazione
D. Modifica dei messaggi

Answer: A
Section: Attacchi attivi

Id Lezione 11: Servizi e meccanismi di sicurezza

1. Quali di queste categorie non fa parte dei servizi di sicurezza:
A. Autenticazione
B. Privacy
C. Integrità dei dati
D. Segretezza dei dati

Answer: B
Section: Servizi di sicurezza: autenticazione e controllo accessi

2. Il servizio di autenticazione garantisce:
A. La riservatezza di una comunicazione
B. Lo scambio di chiavi
C. La segretezza dei dati
D. L'autenticità di una comunicazione

Answer: D
Section: Servizi di sicurezza: autenticazione e controllo accessi

3. Il servizio di controllo degli accessi definisce:
A. Chi può avere accesso a una risorsa, in quali condizioni può farlo e cosa può farne
B. Come impedire gli accessi
C. Quanti utenti possono accedere
D. La politica di invio dei dati

Answer: A
Section: Servizi di sicurezza: autenticazione e controllo accessi

4. Quale servizio si occupa di proteggere il flusso dei dati dall'analisi:
A. Crittografia
B. Segretezza del traffico
C. Autenticazione dell'entità peer
D. Integrità dei dati

Answer: B
Section: Servizi di sicurezza: segretezza, integritÃ , non ripudiabilitÃ

5. Il servizio di Integrità dei dati garantisce che:
A. Il destinatario sia autenticato
B. I dati ricevuti non sono stati modificati
C. Il mittente sia autenticato
D. La comunicazione sia cifrata

Answer: B
Section: Servizi di sicurezza: segretezza, integritÃ , non ripudiabilitÃ

6. Il servizio di Non Ripudiabilità impedisce che:
A. Il messaggio sia modificato
B. Il destinatario conosca il mittente
C. Il mittente possa inviare più messaggi

D. Il mittente neghi di aver inviato il messaggio

Answer: D
Section: Servizi di sicurezza: segretezza, integritÃ , non ripudiabilitÃ

7. I Meccanismi di Sicurezza si dividono in:
A. Specifici e alternativi
B. Generici e pervasivi
C. Specifici e diretti
D. Specifici e pervasivi

Answer: D
Section: Meccanismi di sicurezza

8. Il Controllo dell'Instradamento è:
A. Un Meccanismo di Sicurezza pervasivo
B. Un Meccanismo di Sicurezza orientato alla riduzione dei tempi di trasmissione
C. Un Meccanismo di Sicurezza da utilizzare nel caso si sospetti di essere sottoposti ad attacco in certi punti della rete
D. Un Meccanismo di Sicurezza specifico orientato all'integrità dei dati

Answer: C
Section: Meccanismi di sicurezza

9. I Meccanismi di Sicurezza pervasivi sono:
A. Specifici del servizio di sicurezza
B. Specifici del livello del protocollo
C. Orientati all'autenticazione
D. Applicabili a diversi servizi di sicurezza

Answer: D
Section: Meccanismi di sicurezza

10. Nel modello generale per la sicurezza di rete esistono sempre:
A. Una terza parte fidata
B. Un componente per la trasformazione delle informazioni
C. Un attaccante che intercetta il messaggio
D. Un componente per l'accesso alle informazioni segrete

Answer: B
Section: Un modello per la sicurezza di rete

Id Lezione 12: Crittografia simmetrica

1. Cosa si intende per crittografia simmetrica:
A. Cifratura e decifratura funzionano allo stesso modo
B. Il testo cifrato si presenta simmetrico
C. Cifratura e decifratura usano la stessa chiave
D. Cifratura e decifratura usano due chiavi tra di loro simmetriche

Answer: C
Section: Definizioni di base

2. Cosa si intende col termine criptologia:
A. L''insieme di crittografia e analisi crittografica
B. La cripto-analisi
C. L'insieme delle tecniche di attacco crittografico
D. L'insieme di tecniche per la crittografia

Answer: A
Section: Definizioni di base

3. Quali di questi elementi non fa parte del modello di cifratura simmetrico:
A. Testo cifrato
B. Chiave segreta
C. Terza parte fidata
D. Algoritmo di decrittografia

Answer: C
Section: Definizioni di base

4. Quale delle seguenti affermazioni è vera:
A. L'algoritmo di cifratura deve essere necessariamente segreto
B. L'attaccante non deve conoscere l'algoritmo di decifratura
C. La chiave deve restare segreta
D. L'attaccante non deve conoscere copie testo in chiaro/cifrato

Answer: C
Section: Definizioni di base

5. L'attacco "Testo in chiaro noto" prevede:
A. La conoscenza soltanto dell'algoritmo di cifratura
B. La disponibilità di più testi cifrati
C. La disponibilità di un solo testo cifrato
D. La disponibilità di più coppie di testo in chiaro e cifrato

Answer: D
Section: Crittografia e analisi crittografica

6. L'attacco "Testo in chiaro scelto" prevede:
A. La possibilità per il criptanalista di scegliere il testo in chiaro da cifrare
B. La conoscenza della lunghezza della chiave segreta
C. La possibilità per il criptanalista di scegliere il testo cifrato

D. La possibilità per il criptanalista di scegliere indistintamente il testo cifrato o quello in chiaro

Answer: A
Section: Crittografia e analisi crittografica

7. Nel caso di chiave a 56 bit, l'attacco a forza bruta (106 crittografie/µs), per avere successo, impiega:
A. Circa 10 minuti
B. Circa 10 ore
C. Circa 10 giorni
D. Circa 10 anni

Answer: B
Section: Crittografia e analisi crittografica

8. Nella cifratura di Giulio Cesare che cosa si può dire dell'attacco a forza bruta:
A. Non è efficace
B. La conoscenza della lingua del messaggio dà un vantaggio a questo tipo di attacco
C. Non serve conoscere l'algoritmo di cifratura
D. Funziona ma impiega molto tempo

Answer: B
Section: La cifratura di Giulio Cesare

9. DJBP è un testo cifrato, secondo la cifratura di Giulio Cesare, del seguente testo in chiaro:
A. CAIO
B. CIAO
C. CANE
D. CARO

Answer: B
Section: La cifratura di Giulio Cesare

10. Conoscendo la seguente coppia testo in chiaro/testo cifrato BASE/AZRD secondo la cifratura di Giulio Cesare, determinare la chiave segreta K:
A. 1
B. 26
C. 25
D. 3

Answer: C
Section: La cifratura di Giulio Cesare

Id Lezione 13: Crittografia simmetrica: tecniche di sostituzione e di trasposizione

1. La cifratura monoalfabetica si presenta come:
A. Uguale alla cifratura di Cesare
B. La cifratura di Cesare ma con un numero di chiavi pari a 26!
C. Una cifratura inattaccabile
D. Facile da attaccare anche se non si conosce la natura del testo in chiaro

Answer: B
Section: Tecniche di sostituzione: monoalfabetica e Playfair

2. La cifratura Playfair opera:
A. Sui digrammi
B. Sui trigrammi
C. Su una tabella di cifratura 6x5
D. Sulle singole lettere

Answer: A
Section: Tecniche di sostituzione: monoalfabetica e Playfair

3. Nella cifratura Playfair una coppia di lettere viene:
A. Codificata in una terna di lettere
B. Codificata in una coppia di lettere dipendente dalla posizione relativa di tali lettere nella tabella di cifratura
C. Codificata in più coppie di lettere
D. Codificata in una coppia permutata

Answer: B
Section: Tecniche di sostituzione: monoalfabetica e Playfair

4. La cifratura di Vernam prevede:
A. Una decifratura con un'operazione diversa da quella in cifratura
B. Una chiave lunga quanto il testo in chiaro e un'operazione di OR
C. Una cifratura a blocchi
D. Una chiave lunga quanto il testo in chiaro e un'operazione di XOR

Answer: D
Section: Tecniche di sostituzione: Vernam e One-Time Pad

5. Dato K=1101 e P=1101 determinare il testo cifrato:
A. Il testo cifrato è 0000
B. Il testo cifrato è 0001
C. Il testo cifrato è 1000
D. Il testo cifrato è 1111

Answer: A
Section: Tecniche di sostituzione: Vernam e One-Time Pad

6. La tecnica One-Time Pad è inviolabile in quanto:
A. Non prevede l'uso di chiavi
B. La chiave è usata una sola volta
C. La chiave è molto lunga

D. La chiave è lunga quanto il testo cifrato e usata una sola volta

Answer: D
Section: Tecniche di sostituzione: Vernam e One-Time Pad

7. La tecnica Rail Fence è:
A. Una tecnica basata su macchine a rotazione
B. Una tecnica a trasposizione
C. Una tecnica a sostituzione
D. Una tecnica che usa una cifratura a blocchi

Answer: B
Section: Tecniche di trasposizione e macchine a rotazione

8. Il seguente testo cifrato BOAOTNUNFRUA secondo la tecnica Rail Fence equivale al testo in chiaro:
A. Tanti auguri
B. Buonanotte
C. Buona fortuna
D. Buona serata

Answer: C
Section: Tecniche di trasposizione e macchine a rotazione

9. Il seguente testo cifrato ASTENAIXTIUTTLAY secondo la tecnica di trasposizione a righe (4 righe e chiave K=3124) equivale al testo in chiaro:
A. Tanti saluti a x e y
B. Tanti saluti a te xy
C. Tanti saluti a tutti
D. Salutatemi tutti

Answer: B
Section: Tecniche di trasposizione e macchine a rotazione

10. Quale affermazione è sbagliata:
A. Le macchine a rotazione effettuano una cifratura a flusso
B. Nelle macchine a rotazione il numero di cilindri determina la complessità della cifratura
C. Nelle macchine a rotazione l'input di una cifra non determina un cambiamento di stato della macchina
D. Nelle macchine a rotazione ogni cilindro ha 26 terminali di ingresso e 26 di uscita

Answer: C
Section: Tecniche di trasposizione e macchine a rotazione

Id Lezione 14: La cifratura AES - Advanced Encryption Standard

1. L'algoritmo AES risolve il difetto di 3DES di:
A. Lunghezza chiave ridotta
B. Implementazione software molto lenta
C. Cifratura diversa dalla decifratura
D. Non sicurezza rispetto ad attacchi a forza bruta

Answer: B
Section: AES: origini e valutazioni

2. Quale delle seguenti affermazioni è falsa:
A. NIST richiedeva per AES l'uso di blocchi a 128 bit
B. NIST richiedeva per AES l'uso di chiavi di differente lunghezza
C. L'algoritmo Rijndael fu selezionato per AES
D. L'algoritmo Rijndael si basa sui blocchi di Feistel

Answer: D
Section: AES: origini e valutazioni

3. L'algoritmo AES usa:
A. Una dimensione di blocco di 64 bit
B. Una dimensione di blocco di 128 bit e chiave di 56 bit
C. Una dimensione di blocco di 128 bit e chiave di 128 bit
D. Una dimensione di blocco di 128 bit e chiave di qualsiasi lunghezza

Answer: C
Section: AES: caratteristiche

4. L'algoritmo AES si basa su:
A. Fasi composte da blocchi di Feistel
B. Fasi composte da due funzioni
C. Fasi composte da quattro funzioni
D. Fasi composte da funzioni di permutazione

Answer: C
Section: AES: caratteristiche

5. Nella parametrizzazione di AES, una word corrisponde a:
A. 32 bit
B. 64 bit
C. 128 bit
D. 16 bit

Answer: A
Section: AES: caratteristiche

6. Nella funzione di Byte substitution:
A. Si esegue una permutazione ciclica
B. L'operazione si basa su una S-box composta da 64 valori
C. L'operazione si basa su una S-box composta da 256 valori

D. I primi 4 bit e i secondi 4 bit individuano rispettivamente la colonna e la riga della S-box

Answer: C
Section: Le funzioni di AES

7. Nella funzione di Shift rows:
A. Si eseguono degli spostamenti circolari a destra
B. Si eseguono degli spostamenti circolari a destra e a sinistra
C. Si eseguono degli spostamenti circolari a destra di un byte
D. Si eseguono degli spostamenti circolari a sinistra ma la prima riga non cambia

Answer: D
Section: Le funzioni di AES

8. Nella funzione di Mix columns:
A. Ogni byte generato dipende da tutti e quattro i byte in colonna
B. Ogni byte generato dipende da tutti e quattro i byte nella riga
C. Ogni colonna è elaborata insieme a quella seguente
D. L'output contiene un numero di byte superiori all'input

Answer: A
Section: Le funzioni di AES

9. Nella funzione di Add round key:
A. Viene eseguita una espansione della chiave
B. Si esegue un'operazione di XOR bit a bit tra il testo e la chiave seguita da una permutazione ciclica
C. Si esegue un'operazione di XOR bit a bit tra il testo e la chiave
D. Si esegue un'operazione di XOR bit a bit tra il testo e la chiave ma la chiave ha lunghezza diversa nelle varie fasi

Answer: C
Section: Le funzioni di AES

10. L'espansione della chiave:
A. Espande la chiave da 4 word a 44 word
B. Esegue solo delle operazioni di XOR
C. Espande la chiave da 4 word a 16 word
D. Espande la chiave da 4 word a 44 word ma non tutte vengono poi adoperate

Answer: A
Section: Le funzioni di AES

Id Lezione 15: Modalità di funzionamento della cifratura a blocchi

1. Le modalità di funzionamento della cifratura definiscono:
A. La tipologia di algoritmo da usare
B. Come vengono eseguite in sequenza le operazioni di cifratura
C. Il numero e la dimensione dei blocchi
D. La generazione delle chiavi di cifratura

Answer: B
Section: Modalità di funzionamento della cifratura a blocchi: intro

2. Quale fra le seguenti non è una modalità di cifratura:
A. Cipher Block Chaining
B. Electronic Codebook
C. Output chaining
D. Counter

Answer: C
Section: Modalità di funzionamento della cifratura a blocchi: intro

3. Nella modalità Electronic Codebook non si usa:
A. Sempre la stessa chiave
B. Cifratura e decifratura diverse
C. Bit di riempimento
D. Blocchi di dimensione diversa

Answer: D
Section: Electronic Codebook (ECB)

4. Lo svantaggio principale della modalità Electronic Codebook è:
A. La necessità di usare bit di riempimento
B. L'uso della stessa chiave
C. La semplicità di cifratura
D. Lo stesso blocco di testo in chiaro produce lo stesso blocco di testo cifrato

Answer: D
Section: Electronic Codebook (ECB)

5. Nella modalità Cipher Block Chaining come si risolvono i problemi di sicurezza di ECB:
A. Utilizzando un vettore di inizializzazione
B. Mettendo in input il testo cifrato al passo precedente
C. Cambiando la chiave ad ogni passo
D. Rendendo cifratura e decifratura uguali

Answer: B
Section: Cipher Block Chaining (CBC)

6. Nella modalità Cipher Block Chaining quali requisiti ci sono sul vettore di inizializzazione:
A. Deve essere generato dalla chiave
B. Deve essere cambiato ad ogni passo
C. Deve essere noto al destinatario

D. Nessun requisito

Answer: C
Section: Cipher Block Chaining (CBC)

7. Nella modalità Cipher Feedback cosa viene messo in input alla funzione di crittografia:
A. Un registro a scorrimento di s bit (dimensione segmento) e la chiave K
B. Un registro a scorrimento di b bit (dimensione blocco)e la chiave K
C. Il testo in chiaro e la chiave K
D. Il testo cifrato al passo precedente e la chiave K

Answer: B
Section: Cipher Feedback (CFB)

8. Nella modalità Cipher Feedback il testo in chiaro è in XOR con:
A. Con il vettore di inizializzazione
B. Con il testo cifrato al passo precedente
C. Con gli s bit più significativi del testo in uscita dalla cifratura
D. Con gli s bit meno significativi del testo in uscita dalla cifratura

Answer: C
Section: Cipher Feedback (CFB)

9. Nella modalità Output Feedback cosa cambia rispetto a Cipher Feedback:
A. Nel registro a scorrimento vengono inseriti b bit che escono dalla cifratura al passo precedente e non quelli che escono dallo XOR con il testo in chiaro
B. Nel registro a scorrimento vengono inseriti s bit del testo in chiaro al passo precedente e non quelli che escono dallo XOR con il testo in chiaro
C. Nel registro a scorrimento vengono inseriti s bit che escono dalla cifratura al passo precedente e non quelli che escono dallo XOR con il testo in chiaro
D. Nel registro a scorrimento vengono inseriti s bit che escono dalla cifratura al passo precedente in XOR con la chiave e non quelli che escono dallo XOR con il testo in chiaro

Answer: C
Section: Output Feedback (OFB)

10. Nella modalità Counter, quale di queste affermazioni è sbagliata:
A. Cifratura e decifratura sono la stessa funzione
B. Il valore di ciascun contatore non cambia da blocco a blocco
C. Il valore del contatore viene cifrato e messo in XOR con il testo in chiaro
D. Non esiste alcuna concatenazione tra i vari passi

Answer: B
Section: Counter (CTR)

Id Lezione 16: Segretezza e crittografia simmetrica

1. Nell'uso della crittografia simmetrica in un ambiente distribuito cosa è cruciale definire:
A. Il punto in cui usare la crittografia
B. La lunghezza della chiave
C. La dimensione del blocco
D. La tecnica crittografica

Answer: A
Section: Introduzione

2. In cosa differiscono la crittografia di canale e quella end-to-end:
A. Sono la stessa cosa
B. Nell'uso della chiave segreta
C. Nella crittografia di canale la cifratura viene eseguita tra i terminali finali
D. Nella crittografia end-to-end la cifratura viene eseguita tra i terminali finali

Answer: D
Section: Introduzione

3. La crittografia di canale:
A. Viene eseguita tra ogni collegamento vulnerabile
B. Viene eseguita solo tra alcuni nodi principali di collegamento
C. Viene eseguita solo tra i nodi terminali della trasmissione
D. Viene eseguita a livello alti della gerarchia OSI

Answer: A
Section: Crittografia di canale e end-to-end

4. La principale complessità della crittografia di canale riguarda:
A. Non ci sono complessità
B. La necessità di un grande numero di dispositivi di crittografia e di chiavi
C. La vulnerabilità agli attacchi
D. La dimensione del blocco dati

Answer: B
Section: Crittografia di canale e end-to-end

5. Nella cifratura end-to-end sono protetti:
A. I dati utente sono in chiaro ma il flusso nella rete è protetto
B. I dati utente e il loro flusso
C. Solo una parte dei dati utente
D. I dati utente ma non il loro flusso

Answer: D
Section: Crittografia di canale e end-to-end

6. La cifratura end-to-end viene inserita a:
A. I livelli più bassi della gerarchia OSI
B. I livelli più alti della gerarchia OSI
C. Al livello "fisico" della gerarchia OSI

D. Al livello "collegamento" della gerarchia OSI

Answer: B
Section: Crittografia di canale e end-to-end

7. Quale delle seguenti modalità di distribuzione della chiave segreta non è praticabile:
A. A consegna fisicamente la chiave a B
B. Un KDC consegna fisicamente la chiave ad A e B
C. A sceglie una chiave e la invia a B
D. A e B possiedono già una chiave condivisa e usano quella per scambiarsene una nuova

Answer: C
Section: Distribuzione delle chiavi

8. Nella crittografia end-to-end se ci sono N host che devono scambiarsi dati, quante chiavi sono necessarie:
A. N
B. N/2
C. [N(N-1)]/2
D. N(N-1)

Answer: C
Section: Distribuzione delle chiavi

9. Nel protocollo di distribuzione delle chiavi, perché l'utente A invia un nonce:
A. Per identificare univocamente quella richiesta
B. Per identificarsi
C. Non invia un nonce
D. Per poi inviarlo all'utente B

Answer: A
Section: Un esempio di distribuzione delle chiavi

10. Nel protocollo di distribuzione delle chiavi, cosa contiene il messaggio di risposta del KDC all'utente A:
A. La chiave di sessione
B. La chiave di sessione, il messaggio inviato da A e il messaggio da inviare a B cifrato con la chiave di B
C. La chiave di sessione e il messaggio da inviare a B cifrato con la chiave di B
D. La chiave di sessione e il messaggio da inviare a B cifrato con la chiave di B

Answer: B
Section: Un esempio di distribuzione delle chiavi

Id Lezione 17: Crittografia asimmetrica

1. La crittografia asimmetrica prevede:
A. L'uso di due chiavi segrete
B. L'uso di una chiave segreta
C. L'uso di due chiavi di cui una privata
D. L'uso di due chiavi pubbliche

Answer: C
Section: Concetti base

2. La crittografia asimmetrica nasce per risolvere il problema:
A. Della distribuzione delle chiavi e della firma digitale
B. Di ridurre i tempi computazionali
C. Di aumentare la robustezza
D. Di sostituire la crittografia simmetrica

Answer: A
Section: Concetti base

3. Nella crittografia a chiave pubblica è computazionalmente impraticabile:
A. Calcolare il testo in chiaro dal testo cifrato
B. Ricavare la chiave privata da quella pubblica
C. Calcolare il testo cifrato da quello in chiaro
D. Ricavare la chiave pubblica da quella privata

Answer: B
Section: Sistemi crittografici a chiave pubblica

4. Nel caso di utilizzo della crittografia asimmetrica per la funzione di segretezza:
A. Il mittente usa in cifratura la chiave privata del destinatario
B. Il mittente usa in cifratura la sua chiave pubblica
C. Il mittente usa in cifratura la chiave pubblica del destinatario
D. Il mittente usa in cifratura la sua chiave privata

Answer: C
Section: Sistemi crittografici a chiave pubblica

5. Nel caso di utilizzo della crittografia asimmetrica per la funzione di segretezza, un eventuale attaccante può riuscire a stimare:
A. La chiave pubblica del destinatario
B. Solo il messaggio in chiaro
C. Solo la chiave privata del destinatario
D. La chiave privata del destinatario e il messaggio in chiaro

Answer: D
Section: Sistemi crittografici a chiave pubblica

6. Nel caso di utilizzo della crittografia asimmetrica per la funzione di autenticazione:
A. Il mittente usa in cifratura la chiave pubblica del destinatario
B. Il mittente usa in cifratura la chiave privata del destinatario

C. Il mittente usa in cifratura la propria chiave pubblica
D. Il mittente usa in cifratura la propria chiave privata

Answer: D
Section: Sistemi crittografici a chiave pubblica

7. Nel caso di utilizzo della crittografia asimmetrica per la funzione di autenticazione, un eventuale attaccante può riuscire a stimare:
A. La chiave privata del destinatario
B. Il testo in chiaro
C. La chiave pubblica del mittente
D. La chiave privata del mittente

Answer: D
Section: Sistemi crittografici a chiave pubblica

8. Con la crittografia asimmetrica si riesce a garantire autenticazione e segretezza:
A. NO
B. Sì sempre
C. Sì ma usando entrambe le coppie di chiavi del mittente e del destinatario
D. Sì ma scambiandosi le chiavi private

Answer: C
Section: Sistemi crittografici a chiave pubblica

9. Nella crittografia asimmetrica l'operazione Y=fk(X) deve essere:
A. Facile se X noto
B. Difficile da calcolare
C. Facile se X e K noti
D. Non invertibile

Answer: C
Section: Requisiti della crittografia a chiave pubblica

10. La crittografia asimmetrica è vulnerabile a:
A. Solo ad attacchi ad analisi del traffico
B. Non è vulnerabile
C. Attacchi a forza bruta
D. Solo ad attacchi che stimano la chiave privata

Answer: C
Section: Requisiti della crittografia a chiave pubblica

Id Lezione 18: L'algoritmo RSA

1. La sicurezza dell'algoritmo RSA sta:
A. Nell'uso di una chiave pubblica
B. Nella segretezza delle due chiavi
C. Nella difficoltà dell'operazione di fattorizzazione di grandi numeri
D. Nella difficoltà dell'operazione di fattorizzazione

Answer: C
Section: Descrizione dell'algoritmo

2. In RSA il valore n=p*q è:
A. Pubblico e scelto dall'utente
B. Privato e scelto dall'utente
C. Pubblico e calcolato dall'utente
D. Privato e calcolato dall'utente

Answer: C
Section: Descrizione dell'algoritmo

3. In RSA , a quanto equivale φ(n):
A. P*q
B. (p-1)*(q-1)
C. P*(q-1)
D. (p-1)*(q-1)

Answer: B
Section: Descrizione dell'algoritmo

4. In RSA, qual è il legame tra φ(n) e il valore e:
A. MCD(φ(n),e)=1
B. Nessun legame
C. φ(n)*e=1
D. φ(n)

Answer: A
Section: Descrizione dell'algoritmo

5. In RSA, qual è il legame tra il valore d e il valore e:
A. E>d
B. E*d=1mod(φ(n))
C. E*d=1mod(n)
D. E*d=1

Answer: B
Section: Descrizione dell'algoritmo

6. Quale operazione esegue il destinatario del messaggio cifrato C:
A. Cdmodn=M
B. Cemodn=M
C. Cemod(φ(n))=M

D. (C*d)modn=M

Answer: A
Section: Descrizione dell'algoritmo

7. Quale proprietà dell'aritmetica modulare si usa in RSA nella cifratura/decifratura:
A. [(a mod n)*(b mod n)] mod n =1 mod n
B. [(a mod n)*(b mod n)] mod n =(a*b) mod n
C. [(a mod n)*(b mod n)] mod n =n mod n
D. [(a mod n)*(b mod n)] mod n =ab

Answer: B
Section: Esempio di algoritmo RSA

8. In RSA, cosa permette di fare l'algoritmo di Miller-Rabin:
A. Non serve
B. Determinare φ(n)
C. Determinare n
D. Determinare i numeri primi p e q

Answer: D
Section: La generazione della chiave

9. Quali operazioni complesse deve effettuare un utente in RSA:
A. La scelta dei numeri primi p e q
B. La scelta dei numeri primi n e q
C. La scelta dei numeri primi n e p
D. Nessuna operazione complessa

Answer: A
Section: La generazione della chiave

10. In RSA, cosa permette di fare l'algoritmo di Euclide esteso:
A. Selezionare e o d e calcolare l'altro valore
B. Selezionare n o d e calcolare l'altro valore
C. Calcolare MCD(φ(n),e)
D. Calcolare MCD(d,e)

Answer: A
Section: La generazione della chiave

Id Lezione 19: Autenticazione dei messaggi

1. La firma digitale per l'autenticazione soddisfa il requisito:
A. Ripudio del destinatario
B. Ripudio del mittente
C. Segretezza
D. Ripudio mittente e destinatario

Answer: B
Section: Requisiti per lâ€™autenticazione

2. La crittografia simmetrica può garantire:
A. La firma digitale
B. Segretezza e autenticazione
C. Non ripudiabilità
D. Da sola non dà garanzia

Answer: B
Section: Le funzioni di autenticazione

3. La crittografia asimmetrica che usa in cifratura la chiave pubblica del destinatario può garantire:
A. Autenticazione e segretezza
B. Segretezza ma non autenticazione
C. Autenticazione ma non segretezza
D. Né autenticazione né segretezza

Answer: B
Section: Le funzioni di autenticazione

4. La crittografia asimmetrica che usa in cifratura la chiave privata del mittente può garantire:
A. Autenticazione e segretezza
B. Segretezza ma non autenticazione
C. Autenticazione ma non segretezza
D. Né autenticazione né segretezza

Answer: C
Section: Le funzioni di autenticazione

5. Per garantire segretezza, autenticazione e firma, in cifratura asimmetrica si devono usare:
A. La chiave privata del mittente e poi la chiave pubblica del destinatario
B. La chiave privata del destinatario e poi la chiave pubblica del mittente
C. La chiave pubblica del destinatario e poi la chiave pubblica del mittente
D. La chiave pubblica del destinatario e poi la chiave privata del mittente

Answer: A
Section: Le funzioni di autenticazione

6. Il codice MAC garantisce:
A. La segretezza
B. La firma
C. L'autenticazione

D. L'autenticazione e la segretezza

Answer: C
Section: Il codice MAC

7. Il codice MAC per garantire la segretezza ha bisogno di:
A. Cifratura a chiave pubblica
B. Due chiavi distinte
C. Due chiavi uguali
D. Non può garantire segretezza

Answer: B
Section: Il codice MAC

8. Qual è la differenza sostanziale fra un codice MAC e una funzione hash:
A. Non c'è differenza
B. La funzione hash non dipende da una chiave
C. Il codice MAC non dipende da una chiave
D. La funzione hash è invertibile

Answer: B
Section: La funzione hash

9. La funzione hash, integrata con la cifratura simmetrica, riesce a garantire:
A. La firma digitale
B. Solo l'autenticazione
C. Solo la segretezza
D. L'autenticazione e la segretezza

Answer: D
Section: La funzione hash

10. Con la sola funzione hash si riesce a garantire:
A. La segretezza
B. La firma digitale
C. L'autenticazione ma le due parti devono condividere un valore segreto
D. La segretezza ma le due parti devono condividere un valore segreto

Answer: C
Section: La funzione hash

Id Lezione 20: Le firme digitali

1. Perché è necessaria la firma digitale:
A. Per proteggere il mittente
B. Per proteggere il destinatario
C. Per proteggere la trasmissione di un messaggio
D. Per proteggere il mittente e il destinatario

Answer: D
Section: Requisiti per le firme digitali

2. Quali dei seguenti non è un requisito per la firma digitale:
A. Deve essere indipendente dal messaggio
B. Deve essere verificabile da terzi
C. Deve essere specifica del mittente
D. Deve essere possibile conservare una copia della firma digitale

Answer: A
Section: Requisiti per le firme digitali

3. Nella firma digitale diretta gli attori in gioco sono:
A. Il mittente e il destinatario
B. Il mittente
C. Il destinatario
D. Una terza parte e il mittente

Answer: A
Section: La firma digitale diretta

4. La firma digitale diretta può essere realizzata:
A. Solo con la cifratura a chiave pubblica
B. Solo con la cifratura simmetrica
C. Con la cifratura simmetrica o asimmetrica
D. Con la cifratura simmetrica ma con doppia chiave

Answer: A
Section: La firma digitale diretta

5. Nella firma digitale diretta è possibile usare solo una coppia di chiavi pubblica/privata:
A. No, non è possibile
B. Sì, usando la coppia del destinatario
C. Sì, usando la coppia del mittente e garantendo la segretezza
D. Sì, usando la coppia del mittente ma senza garantire la segretezza

Answer: D
Section: La firma digitale diretta

6. Nella firma digitale diretta, il punto debole è costitito da:
A. La mancanza di una terza parte garante
B. Gestione della chiave del mittente
C. Non c'è un punto debole

D. Dal fatto che non c'è segretezza nella trasmissione

Answer: B
Section: La firma digitale diretta

7. La firma digitale arbitrata garantisce:
A. Un'altra modalità di firma digitale
B. Una modalità di firma digitale più sicura di quella diretta
C. Una modalità di firma digitale meno sicura di quella diretta
D. Una modalità di firma digitale in cui può essere presente un arbitro

Answer: A
Section: La firma digitale arbitrata

8. Nella firma digitale arbitrata con chiave simmetrica si ha che:
A. Il mittente e il destinatario condividono la stessa chiave
B. Il mittente e il destinatario condividono la stessa chiave e ciascuno di loro una chiave diversa con l'arbitro
C. Il mittente e il destinatario condividono la stessa chiave e ciascuno di loro una chiave uguale con l'arbitro
D. Il mittente e il destinatario condividono una chiave diversa con l'arbitro

Answer: B
Section: La firma digitale arbitrata

9. Nella firma digitale arbitrata con chiave simmetrica si ha che:
A. L'arbitro legge il messaggio
B. L'arbitro invia al mittente la chiave di sessione
C. L'arbitro non legge il messaggio
D. L'arbitro invia al destinatario la chiave di sessione

Answer: C
Section: La firma digitale arbitrata

10. Nella firma digitale arbitrata con chiave simmetrica si ha che:
A. L'arbitro aggiunge un timestamp alla firma del mittente
B. L'arbitro aggiunge la sua firma alla firma del mittente
C. L'arbitro aggiunge il suo identificativo alla firma del mittente
D. L'arbitro invia una chiave di sessione al mittente e al destinatario

Answer: A
Section: La firma digitale arbitrata

Id Lezione 21: Sicurezza della posta elettronica e PGP

1. PGP è uno standard per la posta elettronica basata su:
A. Cifratura RSA
B. Hash SHA-1
C. Cifratura simmetrica 3DES
D. Cifratura pubblica, cifratura simmetrica e hash.

Answer: D
Section: PGP: introduzione

2. Nel PGP la compatibilità con le funzionalità di posta elettronica sono garantite attraverso:
A. L'algoritmo ZIP
B. La decifratura simmetrica
C. La conversione ASCII radix-64
D. La decifratura asimmetrica

Answer: C
Section: PGP: introduzione

3. In PGP, l'autenticazione viene garantita tramite:
A. La cifratura simmetrica e l'algoritmo ZIP
B. Hash SHA-1 e la cifratura simmetrica
C. Hash SHA-1 e la cifratura asimmetrica
D. La cifratura simmetrica

Answer: C
Section: PGP: autenticazione

4. In PGP, l'autenticazione non garantisce:
A. La compressione
B. La segretezza
C. La firma digitale
D. La provenienza del messaggio

Answer: B
Section: PGP: autenticazione

5. In PGP, la segretezza è fornita attraverso:
A. La cifratura simmetrica
B. La cifratura asimmetrica
C. Hash SHA-1
D. La compressione ZIP

Answer: A
Section: PGP: segretezza

6. In PGP, la chiave simmetrica è trasferita usando:
A. La cifratura simmetrica
B. La cifratura asimmetrica
C. Non viene trasferita

D. Hash SHA-1

Answer: B
Section: PGP: segretezza

7. In PGP, si realizza autenticazione e segretezza tramite:
A. La chiave privata del mittente, la chiave segreta di sessione e la chiave pubblica del destinatario
B. La chiave privata del mittente e la chiave pubblica del destinatario
C. La chiave privata del mittente e la chiave segreta di sessione
D. Non è realizzabile

Answer: A
Section: PGP: segretezza

8. In PGP, la compressione ZIP si effettua:
A. Dopo aver applicato la crittografia simmetrica
B. Dopo aver applicato la firma ma prima della crittografia simmetrica
C. Non si applica
D. Dopo aver applicato la crittografia simmetrica ma prima della firma

Answer: B
Section: PGP: compressione, compatibilitÃ e frammentazione

9. In PGP, la conversione radix-64 determina:
A. Un aumento della dimensione del messaggio
B. Una decifratura del messaggio
C. Un rallentamento
D. Una conversione byte a byte

Answer: A
Section: PGP: compressione, compatibilitÃ e frammentazione

10. In PGP, la conversione radix-64 trasforma:
A. Un gruppo di 8 bit in un carattere ASCII
B. Un gruppo di 6 bit in altri 6 bit permutati
C. Un gruppo di 16 bit in un carattere ASCII
D. Un gruppo di 6 bit in un carattere ASCII

Answer: D
Section: PGP: compressione, compatibilitÃ e frammentazione

Id Lezione 22: SET - Secure Electronic Transaction

1. Nello standard SET la segretezza del pagamento e dell'ordine è garantita tramite:
A. Cifratura RSA
B. Hash SHA-1
C. Cifratura simmetrica DES
D. Cifratura a chiave pubblica.

Answer: C
Section: SET: introduzione

2. Nello standard SET l'integrità dei dati trasmessi è garantita attraverso:
A. Cifratura simmetrica DES
B. La firma digitale basata su RSA e i codici hash SHA-1
C. Cifratura simmetrica 3DES
D. La codifica hash SHA-1

Answer: B
Section: SET: introduzione

3. Nello standard SET, il venditore dialoga:
A. Solo con il cliente
B. Solo con la banca del cliente
C. Con il cliente e il gateway di pagamento
D. Solo con il gateway di pagamento

Answer: C
Section: SET: introduzione

4. Nello standard SET, la doppia firma serve a:
A. A collegare due messaggi per due diversi destinatari ma provenienti da stesso mittente
B. Ad inviare le informazioni dell'ordine
C. Ad inviare le informazioni del pagamento
D. A garantire il venditore

Answer: A
Section: Doppia firma

5. Nello standard SET, la doppia firma DS è ottenuta:
A. E(PRC,H[H(PI)||H(OI)])
B. E(PRC,H(PI))
C. E(PRC,H(OI))
D. H[H(PI)||H(OI)]

Answer: A
Section: Doppia firma

6. Nello standard SET, per verificare la doppia firma il venditore e la banca eseguono una stessa operazione:
A. Nessuna operazione comune
B. L'hash delle informazioni dell'ordine
C. La decifratura della doppia firma con la chiave pubblica del cliente

D. La decifratura della doppia firma con la chiave privata del cliente

Answer: C
Section: Doppia firma

7. Nella Purchase Request dello standard SET, il cliente invia:
A. Una chiave simmetrica monouso cifrata con la chiave pubblica del venditore
B. Una chiave simmetrica monouso cifrata con la chiave pubblica del gateway di pagamento
C. Una chiave simmetrica monouso non cifrata
D. Una chiave simmetrica monouso cifrata con un hash

Answer: B
Section: Pagamenti: richiesta di acquisto

8. Nella Purchase Response dello standard SET, il venditore invia:
A. Un blocco di conferma cifrato con la chiave pubblica del gateway di pagamento
B. Un blocco di conferma cifrato con la sua chiave pubblica
C. Un blocco di conferma cifrato con la sua chiave privata
D. Un blocco di conferma cifrato con la chiave monouso inviata dal cliente

Answer: C
Section: Pagamenti: richiesta di acquisto

9. Nella fase di Authorization Request dello standard SET, il venditore invia al gateway di pagamento:
A. Nessuna chiave simmetrica
B. Una chiave simmetrica monouso diversa da quella inviatagli dal cliente
C. Una chiave simmetrica monouso uguale a quella inviatagli dal cliente
D. La propria chiave privata

Answer: B
Section: Pagamenti: autorizzazione del pagamento

10. Nello standard SET, la fase di cattura del pagamento avviene tra:
A. Il venditore e il cliente
B. Il venditore e l'emettitore
C. Il venditore e il gateway di pagamento
D. Il cliente e il gateway di pagamento

Answer: C
Section: Pagamenti: cattura del pagamento

Id Lezione 23: Intrusioni e software doloso

1. Con il termine "intrusione" si intende:
A. Un accesso non consentito ad un server
B. Un accesso non consentito ad un sistema e alla informazioni in esso contenute
C. Un accesso non consentito ad una applicazione
D. Un accesso non consentito ad un documento

Answer: B
Section: Intrusioni

2. Il file delle password generalmente contiene:
A. Le password cifrate
B. Nome utente cifrato e password in chiaro
C. Nome utente e password in chiaro
D. Nome utente e password cifrata

Answer: D
Section: Intrusioni

3. Con il termine "malware" si intende:
A. Un virus informatico
B. Un programma nascosto all'interno di un altro o indipendente, creato per compiere azioni illegittime e dannose
C. Un attacco informatico
D. Un programma infettato

Answer: B
Section: Software doloso

4. Quando un malware si replica effettua:
A. La copia di un file infetto
B. La copia di se stesso sullo stesso computer o su altri
C. La copia di se stesso sullo stesso disco
D. Un'azione di attacco informatico

Answer: B
Section: Software doloso

5. Quale delle seguenti affermazioni è falsa:
A. Tutti i malware sono programmi software
B. Tutti i malware devono essere trasferiti in un sistema
C. Tutti i malware si replicano
D. Non sempre i malware compiono azioni dannose sui file

Answer: C
Section: Software doloso

6. Quale di questi malware è specifico della posta elettronica:
A. Bomba logica
B. Worm
C. Virus

D. Spammer

Answer: D
Section: Software doloso

7. Quale dei seguenti malware non è in realtà un software:
A. Backdoor
B. Worm
C. Virus
D. Trojan

Answer: A
Section: Software doloso

8. Un virus è un programma che:
A. Non è un programma
B. Modifica altri programmi e contenuti eseguibili alterandoli; effettua copie di se stesso
C. Non effettua copie di se stesso
D. Si propaga tramite la posta elettronica

Answer: B
Section: I virus

9. La fase di propagazione del virus coincide con:
A. L'avvio della sua azione dolosa
B. Lo svolgimento della sua azione dolosa
C. L'inserimento di copie di se stesso in altri programmi, dischi o memorie
D. La replica di file infetti

Answer: C
Section: I virus

10. Con il termine "virus polimorfico" si intende:
A. Un virus che attacca file di tipo diverso
B. Un virus che quando si replica modifica il suo aspetto e la sua tipologia di attacco
C. Un virus che quando si replica non modifica il suo aspetto pur eseguendo diversi tipi di attacco
D. Un virus che quando si replica modifica il suo aspetto ma esegue la stessa tipologia di attacco

Answer: D
Section: I virus

Id Lezione 24: Cifratura a blocchi

1. La cifratura a blocchi è:
A. Più vantaggiosa di quella a flussi
B. Più complessa di quella a flussi
C. Basata sull'elaborazione di un blocco di testo in chiaro
D. Dipendente solo da sottoparti della chiave

Answer: C
Section: Principi della cifratura a blocchi

2. La cifratura a blocchi ideale non è praticabile perché:
A. Dovrebbe avere risorse infinite per la cifratura
B. Lo spazio delle chiavi possibili sarebbe limitato
C. Non sarebbe comunque sicura
D. La chiave sarebbe molto lunga

Answer: D
Section: Principi della cifratura a blocchi

3. La cifratura di Feistel:
A. Usa una chiave molto lunga
B. Usa un numero elevato di fasi
C. Usa una dimensione del blocco e della chiave praticabile
D. Usa algoritmi diversi in cifratura e decifratura

Answer: C
Section: La cifratura di Feistel

4. La cifratura di Feistel mette in pratica i concetti di:
A. Sostituzione e confusione
B. Diffusione e sostituzione
C. Diffusione e confusione
D. Diffusione e permutazione

Answer: C
Section: La cifratura di Feistel

5. Nella cifratura di Feistel cosa accade tra una fase e la successiva:
A. La parte REi viene sostituita nella parte LEi+1
B. La parte REi+1 viene sostituita nella parte LEi+1
C. La parte REi+1 viene sostituita nella parte LEi
D. La parte REi+1 viene permutata

Answer: A
Section: La cifratura di Feistel

6. Nella cifratura di Feistel accade che:
A. Ogni fase usa la stessa sottochiave
B. La parte LEi va in XOR con F(REi, Ki+1)
C. La parte REi va in XOR con F(LEi, Ki+1)

D. La parte LEi va in XOR con REi

Answer: B
Section: La cifratura di Feistel

7. Nella decifratura di Feistel si ha che:
A. Le sottochiavi sono in numero minore rispetto alla cifratura
B. Le sottochiavi si usano in ordine inverso
C. Le sottochiavi si usano nel medesimo ordine
D. Le sottochiavi si usano in ordine inverso e permutate

Answer: B
Section: La cifratura di Feistel

8. Nella decifratura di Feistel quale delle seguenti proprietà permette la generazione del corretto input della fase (i-1)-esima:
A. F(REi-1, Ki) $\oplus$ F(REi-1, Ki)=0
B. F(REi-1, Ki) $\oplus$ F(REi-1, Ki)=REi-1
C. F(REi-1, Ki) $\oplus$ F(REi-1, Ki)=Ki
D. F(REi-1, Ki) $\oplus$ F(REi-1, Ki)=1

Answer: A
Section: La cifratura di Feistel

9. Quale di queste affermazioni sulla nascita del DES non è corretta:
A. Deriva da un algoritmo di nome LUCIFER
B. Si basava sull'uso di strutture S-box
C. Si basava sull'uso di blocchi di Feistel
D. Usava una cifratura diversa dalla decifratura

Answer: D
Section: Cenni storici sul DES

10. Uno dei principali dubbi su DES riguardava:
A. La ridotta dimensione del blocco dati
B. La ridotta dimensione della lunghezza della chiave
C. La ridotta dimensione della chiave rispetto a quello dell'algoritmo iniziale
D. La complessità computazionale

Answer: C
Section: Cenni storici sul DES

Id Lezione 25: La cifratura DES: Data Encryption Standard

1. L'algoritmo DES riceve in input:
A. Blocco dati di 64 bit e chiave di 128 bit
B. Blocco dati di 56 bit e chiave di 56 bit
C. Blocco dati di 64 bit e chiave di 56 bit
D. Blocco dati di 56 bit e chiave di 128 bit

Answer: C
Section: L'algoritmo DES

2. L'algoritmo DES:
A. Si basa sulla cifratura di Feistel
B. Esegue una cifratura a flusso
C. Non esegue permutazioni
D. Usa 56 sottochiavi

Answer: A
Section: L'algoritmo DES

3. Nell'algoritmo DES i dati subiscono una permutazione iniziale:
A. Basata sulla chiave di 56 bit
B. Basata su una sottochiave
C. Basata su una tabella
D. Circolare a sinistra

Answer: C
Section: L'algoritmo DES

4. I 64 bit in input a ciascuna fase:
A. Vengono divisi in due metà, di cui una non viene elaborata ma solo scambiata di posto
B. Vengono divisi in due metà che subiscono la stessa elaborazione
C. Vengono divisi in due metà, di cui una non cambia di posizione
D. Non vengono divisi in due metà

Answer: A
Section: DES: Dettaglio di una fase

5. In ciascuna fase la parte R_{i-1}:
A. Viene inizialmente espansa a 56 bit
B. Non viene elaborata
C. Viene inizialmente espansa a 48 bit e permutata
D. Viene inizialmente espansa ma non permutata

Answer: C
Section: DES: Dettaglio di una fase

6. In ciascuna fase la parte R_{i-1}:
A. Va in XOR con la sottochiave Ki
B. Va in XOR con la sottochiave Ki-1
C. Dopo essere stata espansa e permutata va in XOR con la sottochiave Ki

D. Dopo essere stata espansa e permutata va in XOR con l'altra metà

Answer: C
Section: DES: Dettaglio di una fase

7. Nella funzione S-box i 6 bit di input sono così usati nella tabella di permutazione:
A. Il 1° e il 6° indicano la colonna, mentre quelli dal 2° al 5° individuano la riga
B. Il 1° e il 2° indicano la riga, mentre quelli dal 3° al 6° individuano la colonna
C. Il 5° e il 6° indicano la riga, mentre quelli dal 1° al 4° individuano la colonna
D. Il 1° e il 6° indicano la riga, mentre quelli dal 2° al 5° individuano la colonna

Answer: D
Section: DES: Dettaglio di una fase

8. Nella generazione della chiave DES:
A. 8 bit dei 64 sono scartati casualmente
B. 8 bit dei 64 che si trovano nelle posizioni multiple di 8 sono scartati
C. Nessun bit viene scartato
D. I primi 8 bit sono scartati

Answer: B
Section: Generazione della chiave

9. I 56 bit della chiave DES:
A. Sono divisi in due metà ciascuna delle quali subisce delle trasformazioni indipendenti
B. Sono divisi in due metà ciascuna delle quali subisce le stesse trasformazioni
C. Sono divisi in due metà una delle quali non subisce trasformazioni
D. Sono divisi in due metà ma il risultato della permutazione ottenuta è lo stesso

Answer: A
Section: Generazione della chiave

10. Con il termine "effetto valanga" si intende.:
A. L'aumento di complessità di un algoritmo di crittografia
B. Testi in chiaro che differiscono di pochi bit sono codificati in testi cifrati molto diversi fra loro seppur codificati con la stessa chiave
C. Testi in chiaro che differiscono di pochi bit sono codificati in testi cifrati molto diversi fra loro se codificati con una chiave diversa
D. Testi in chiaro identici sono codificati in testi cifrati molto diversi fra loro seppur codificati con la stessa chiave

Answer: B
Section: Effetto valanga e potenza del DES

Id Lezione 26: La crittografia multipla

1. La crittografia multipla consiste in:
A. Applicare più volte la stessa chiave
B. Applicare più volte l'algoritmo di cifratura ma non di decifratura
C. Applicare più volte uno stesso algoritmo
D. Applicare in sequenza algoritmi di cifratura diversi

Answer: C
Section: La crittografia multipla: 2DES

2. Nella cifratura 2DES si ha che:
A. Le due chiavi sono usate in ordine inverso in cifratura e decifratura
B. Le due chiavi possono essere usate in qualsiasi ordine in cifratura e decifratura
C. Le due chiavi sono usate nello stesso ordine in cifratura e decifratura
D. Le due chiavi hanno lunghezza di 112 bit

Answer: A
Section: La crittografia multipla: 2DES

3. Il vantaggio di usare la cifratura multipla sta:
A. Nell'aumentare la velocità dell'operazione di decifratura
B. Nel poter riutilizzare l'algoritmo base estendendone la sicurezza
C. Nessun vantaggio
D. Nell'aumentare la velocità dell'operazione di cifratura

Answer: B
Section: La crittografia multipla: 2DES

4. Indicare quale relazione implicherebbe la riduzione ad una sola fase nel 2DES:
A. E(K2,E(K1,P))=E(K1,P)
B. E(K2,E(K1,P))=E(K3,P)
C. D(K2,E(K1,P))=E(K3,P)
D. E(K2,E(K1,P))=C

Answer: B
Section: La crittografia multipla: 2DES

5. Indicare quale relazione descrive l'Attacco MitM:
A. E(K1,P)=D(K2,C)
B. E(K1,P)=D(K1,C)
C. E(K2,P)=D(K2,C)
D. E(K1,P)=E(K2,C)

Answer: A
Section: La crittografia multipla: Attacco MitM

6. Nell'Attacco MitM si suppone di:
A. Conoscere una coppia (P, C) e una chiave
B. Conoscere almeno una chiave
C. Conoscere almeno una coppia (P, C)

D. Non conoscere niente

Answer: C
Section: La crittografia multipla: Attacco MitM

7. Nell'Attacco MitM si confrontano:
A. Tutti i possibili testi cifrati con K2 a partire da P con i corrispettivi testi decifrati con K1 a partire da C
B. Tutti i possibili testi cifrati con K1 a partire da P con i corrispettivi testi decifrati con K1 a partire da C
C. Tutti i possibili testi cifrati con K1 a partire da P con i corrispettivi testi decifrati con K2 a partire da C
D. Solo due testi cifrati con K2 e K1 a partire da P

Answer: C
Section: La crittografia multipla: Attacco MitM

8. Quale delle seguenti affermazioni non è vera:
A. Il 3DES usa un'operazione di decifratura durante la cifratura
B. Il 3DES può usare anche due sole chiavi
C. Il 3DES applica tre volte il DES
D. Il 3DES è vulnerabile all'Attacco MitM

Answer: D
Section: La crittografia multipla: 3DES

9. Indicare l'espressione corretta per la cifratura 3DES:
A. C=E(K1,D(K2,E(K1,P)))
B. C=E(K1,E(K2,E(K1,P)))
C. C=E(K1,D(K2,E(K2,P)))
D. C=E(K1,D(K1,E(K1,P)))

Answer: A
Section: La crittografia multipla: 3DES

10. Quale delle seguenti espressioni identifica la compatibilità tra 3DEs e DES:
A. C=E(K1,D(K1,E(K1,P)))
B. C=E(K1,E(K1,E(K1,P)))
C. C=E(K1,D(K1,E(K1,C)))
D. C=E(K1,E(K1,P))

Answer: A
Section: La crittografia multipla: 3DES

Id Lezione 27: Autenticazione in ambienti distribuiti

1. Il protocollo Kerberos V4, in una autenticazione client-server, si basa su:
A. Tanti server di autenticazione distribuiti
B. Un server di autenticazione centralizzato
C. Due server di autenticazione centralizzati
D. Nessun server di autenticazione

Answer: C
Section: Kerberos v4: i passaggi

2. I server di autenticazione svolgono la funzione di:
A. Garantire i server
B. Garantire utenti e server
C. Garantire gli utenti
D. Garantire l'integrità dei dati

Answer: B
Section: Motivazioni

3. In Kerberos V4 il TGS ha la funzione di:
A. Autenticare l'utente in una sessione
B. Consentire all'utente di accedere ad un altro servizio all'interno della stessa sessione
C. Consentire all'utente di accedere ad un'altra sessione senza reimmettere la password
D. Custodire le password degli utenti

Answer: B
Section: Kerberos v4: i passaggi

4. In Kerberos V4, la risposta dell'AS alla richiesta del client è:
A. Cifrata con cifratura simmetrica
B. Cifrata con cifratura asimmetrica
C. Non cifrata
D. Cifrata con cifratura simmetrica ma il client non può decifrarla

Answer: A
Section: Kerberos v4: i passaggi (Fase A)

5. In Kerberos V4, la risposta dell'AS alla richiesta del client contiene fondamentalmente:
A. La chiave Kc,tgs
B. La chiave Kc,tgs e il Tickettgs
C. La chiave Kc
D. Il Tickettgs

Answer: B
Section: Kerberos v4: i passaggi (Fase A)

6. In Kerberos V4, il Ticket_{tgs} è cifrato con:
A. La chiave segreta del server TGS
B. La chiave pubblica del server TGS
C. La chiave privata del client

D. La chiave Kc,tgs

Answer: A
Section: Kerberos v4: i passaggi (Fase A)

7. In Kerberos V4, l'AutenticatoreC inviato dal client al TGS è cifrato con:
A. La chiave segreta del server TGS
B. La chiave Kc,tgs
C. La chiave pubblica del server TGS
D. La chiave privata del client

Answer: B
Section: Kerberos v4: i passaggi (Fase B)

8. In Kerberos V4, il server TGS invia al client:
A. La chiave per dialogare con il server
B. Il Ticket per il server
C. La chiave per dialogare con il server e il Ticket per il server
D. L'ID del server

Answer: C
Section: Kerberos v4: i passaggi (Fase B)

9. In Kerberos V4, il TicketV per il server contiene:
A. La chiave di dialogo tra client e server
B. Nessuna chiave
C. L'AutenticatoreC del client
D. La chiave pubblica del client

Answer: A
Section: Kerberos v4: i passaggi (Fase C)

10. In Kerberos V4, il server, per garantire reciproca autenticazione, può inviare al client:
A. Un timestamp cifrato con la sua chiave privata
B. Il timestamp inviato dal client, incrementato di 1 e cifrato con la chiave tra loro condivisa
C. Il timestamp inviato dal client incrementato di 1 non cifrato
D. Un timestamp cifrato con la chiave tra loro condivisa

Answer: B
Section: Kerberos v4: i passaggi (Fase C)

Id Lezione 28: Tipi di malware e DDoS

1. La caratteristica principale dei worm è:
A. Usare la posta elettronica per diffondersi
B. Non utilizzare le connessioni di rete
C. Propagarsi in maniera attiva
D. Usare i media digitali per diffondersi

Answer: C
Section: I worm

2. In quale modo un worm decide come propagarsi:
A. Sceglie prima le macchine vicine geograficamente
B. Sulla base delle vulnerabilità
C. Sulla base di una temporizzazione
D. Scansionando la rete sulla base di criteri predefiniti dall'hacker

Answer: D
Section: I worm

3. La Bomba Logica costituisce nello specifico:
A. Un malware che si propaga tramite la posta elettronica
B. Un virus indipendente
C. Un attacco informatico
D. Il codice incorporato in un malware e programmato per attivarsi

Answer: D
Section: Altre tipologie di malware

4. Con il termine Cavallo di Troia si indica un malware:
A. All'interno di un altro programma apparentemente innocuo
B. All'interno di un altro malware
C. Una serie di malware
D. Una rete di malware

Answer: A
Section: Altre tipologie di malware

5. Quale dei seguenti non è un malware vero e proprio:
A. Worm
B. Spyware
C. Backdoor
D. Trojan

Answer: C
Section: Altre tipologie di malware

6. Quale delle seguenti definizioni descrive meglio il Backdoor:
A. Servizio di rete
B. Punto di accesso segreto di un programma che viene individuato da un hacker
C. Punto di accesso con livello più basso di segretezza verso un sistema

D. Punto di accesso verso un programma conosciuto da pochi

Answer: B
Section: Altre tipologie di malware

7. Il malware Rootkit permette:
A. Di accedere con profilo root su un certo sistema
B. Di mantenere coperto un accesso illecito con profilo root su un certo sistema
C. Di distribuire illecitamente i privilegi di root di un sistema
D. Di bloccare l'accesso root ad un sitema

Answer: B
Section: Altre tipologie di malware

8. Il malware Keylogger è in grado di:
A. Leggere il file system del sistema attaccato
B. Inibire l'inserimento dati da tastiera
C. Di catturare login e password di un utente sotto attacco
D. Di catturare i caratteri inseriti da tastiera

Answer: D
Section: Altre tipologie di malware

9. Un attacco DDoS cerca di minare:
A. Le risorse interne di un server e/o le risorse di rete verso un certo servizio
B. Le risorse interne di un server ma non le risorse di rete verso un certo servizio
C. L'accesso di un utente verso un certo servizio
D. I file system di più sistemi interconnessi

Answer: A
Section: Attacchi DDoS

10. Nell'attacco DDoS di tipo SYN flood si inviano pacchetti TCP/IP SYN:
A. Con indirizzo del sistema target corretto ma senza indirizzo di ritorno
B. Con indirizzo del sistema target corretto ma indirizzo di ritorno errato
C. Con indirizzo di ritorno uguale a quello del target
D. Con indirizzo del sistema target errato

Answer: B
Section: Attacchi DDoS

Id Lezione 29: I firewall

1. Il firewall si frappone tra:
A. Due host
B. La rete interna e Internet
C. Un host e la rete interna
D. Ogni macchina in comunicazione

Answer: B
Section: Firewall: i principi base

2. Il principale scopo del firewall è:
A. Proteggere la rete interna da eventuali attacchi esterni
B. Proteggere la rete interna da eventuali attacchi interni
C. Proteggere un singolo host della rete interna da eventuali attacchi
D. Proteggere due host reciprocamente

Answer: A
Section: Firewall: i principi base

3. Il firewall monitora il traffico dati:
A. In ingresso
B. In uscita
C. In ingresso e in uscita
D. In ingresso e in uscita solo da alcuni host

Answer: C
Section: Firewall: le caratteristiche

4. Il firewall non può effettuare filtraggio del traffico sulla base di:
A. Indirizzi IP
B. Tipologie di applicazioni
C. Tipologie di contenuti
D. Dati provenienti da reti wireless

Answer: D
Section: Firewall: le caratteristiche

5. Il firewall è in grado di fornire anche:
A. Protezione da attacchi interni
B. Un punto di osservazione di eventi relativi alla sicurezza della rete interna
C. Nient'altro che una barriera di sicurezza
D. Protezione da documenti infettati da virus

Answer: B
Section: Firewall: le caratteristiche

6. Il firewall a filtraggio di pacchetti IP può operare:
A. A livello di applicazione
B. A livello fisico
C. A livello di indirizzi sorgente/destinazione

D. Ad ogni livello

Answer: C
Section: Tipi di firewall

7. La regola di firewall a filtraggio di pacchetti con Direzione=Out, Protocollo=TCP, Porta Dest= >1023 consente:
A. Traffico dati in uscita per il protocollo TCP su una porta di uscita superiore a 1023
B. Traffico dati in entrata per il protocollo TCP su una porta di ingresso superiore a 1023
C. Traffico dati in uscita per il protocollo TCP su indirizzi IP superiore a 1023
D. Traffico dati in uscita per il protocollo TCP uguale a un Kbyte

Answer: A
Section: Tipi di firewall

8. Quale tipo di firewall esercita il filtraggio sulla base delle applicazioni consentite:
A. A pacchetti
B. Proxy a livello di applicazione
C. A ispezione di stati
D. Controllo indirizzi IP

Answer: B
Section: Tipi di firewall

9. La sicurezza multilivello indica:
A. Una politica di sicurezza a strati
B. Una politica di sicurezza in cui le informazioni sono accessibili sulla base di diversi livelli gerarchici
C. Una politica di sicurezza con controlli gerarchici
D. Una politica di sicurezza che implica più livelli di controllo

Answer: B
Section: Sicurezza multilivello

10. Cosa permette la proprietà "no write down":
A. Un soggetto di livello 3 non può leggere in un documento di livello 2
B. Un soggetto di livello 2 non può leggere in un documento di livello 3
C. Un soggetto di livello 2 non può scrivere in un documento di livello 3
D. Un soggetto di livello 3 non può scrivere in un documento di livello 2

Answer: C
Section: Sicurezza multilivello

Id Lezione 30: Gestione delle chiavi e scambio Diffie-Hellman

1. Uno dei principali usi della crittografia asimmetrica è:
A. La cifratura di messaggi
B. La distribuzione di certificati
C. La distribuzione delle chiavi pubbliche
D. La distribuzione delle chiavi segrete

Answer: D
Section: Distribuzione delle chiavi pubbliche

2. La distribuzione delle chiavi pubbliche non avviene:
A. Mediante certificati
B. Mediante la crittografia simmetrica
C. Mediante un'autorità di distribuzione
D. Attraverso l'inserimento in un elenco pubblico

Answer: B
Section: Distribuzione delle chiavi pubbliche

3. Nella distribuzione delle chiavi pubbliche, quale vantaggio dà usare i certificati rispetto al caso di adottare un'autorità di distribuzione:
A. Evita interazioni continue con l'autorità di distribuzione
B. Nessun vantaggio
C. Evita di doversi scambiare le chiavi pubbliche
D. Non ci sono autorità di garanzia

Answer: A
Section: Distribuzione delle chiavi pubbliche

4. Nella distribuzione delle chiavi segrete, si usa la crittografia asimmetrica perché:
A. Poi si può usare la crittografia simmetrica che è più veloce
B. Non è vero, si fa l'opposto
C. Poi si può usare la crittografia simmetrica che è più sicura
D. Non ci sono altri modi per scambiarsi le chiavi segrete

Answer: A
Section: Distribuzione delle chiavi segrete

5. Nella distribuzione semplice della chiave segreta fra due utenti A e B, cosa invia l'utente A all'utente B per iniziare il dialogo:
A. La sua chiave privata e il suo identificativo
B. La sua chiave pubblica
C. La sua chiave pubblica e il suo identificativo
D. La sua chiave pubblica e la chiave segreta di sessione da lui generata

Answer: C
Section: Distribuzione delle chiavi segrete

6. Nella distribuzione semplice della chiave segreta fra due utenti A e B, cosa invia l'utente B all'utente A in risposta al primo invio dell'utente A:

A. La chiave segreta di sessione da lui (utente B) generata
B. La chiave segreta di sessione da lui (utente B) generata, cifrata con la sua chiave privata
C. La chiave segreta di sessione da lui (utente B) generata, cifrata con la chiave pubblica dell'utente A
D. La chiave segreta di sessione da lui (utente B) generata, cifrata con la sua chiave pubblica

Answer: C
Section: Distribuzione delle chiavi segrete

7. Lo scambio di chiavi Diffie-Hellman è reso sicuro da:
A. L'uso di una chiave molto lunga
B. L'uso della crittografia pubblica
C. La difficoltà nel calcolo dei logaritmi discreti
D. La difficoltà nel calcolo di esponenziali

Answer: C
Section: Lo scambio di chiavi Diffie-Hellman

8. Nello scambio di chiavi Diffie-Hellman, i valori q e a sono:
A. Primi fra loro
B. Il valore q è un numero primo e a è un valore intero
C. Due valori primi
D. Il valore q è un numero primo e a è un valore casuale

Answer: B
Section: Lo scambio di chiavi Diffie-Hellman

9. Nello scambio di chiavi Diffie-Hellman, i valori q e a sono:
A. Entrambi pubblici
B. Solo uno dei due è pubblico
C. Il valore q è pubblico ma a è privato
D. Entrambi privati

Answer: A
Section: Lo scambio di chiavi Diffie-Hellman

10. Nello scambio di chiavi Diffie-Hellman, con un attacco a forza bruta l'attaccante dovrebbe calcolare Ya = a (Xa) mod q conoscendo:
A. Ya
B. Ya, il valore a e il valore q
C. Ya e il valore q
D. Ya, Xa e il valore q

Answer: B
Section: Lo scambio di chiavi Diffie-Hellman

Id Lezione 31: Codici MAC e funzioni hash

1. Un codice MAC è caratterizzato da una funzione del tipo:
A. MAC=C(M)
B. MAC=C(K||M)
C. MAC=C(K,M)
D. MAC=C(K, XOR(K,M))

Answer: C
Section: I codici MAC

2. La funzione usata per il codice MAC è:
A. Due-a-uno
B. Uno-a-uno
C. Molti-a-uno
D. Uno-a-molti

Answer: C
Section: I codici MAC

3. Supponiamo di avere un codice MAC con una chiave lunga k=64 bit e un checksum lungo n=16 bit, quante coppie messaggio-checksum dovrebbe conoscere in media un attaccante per riuscire a individuare la chiave con un attacco a forza bruta:
A. 64
B. 4
C. 16
D. 256

Answer: B
Section: I codici MAC

4. Nel caso di MAC basato su crittografia DES e CBC, il checksum di uscita è costituito da:
A. L'output della cifratura DES applicata allo XOR fra l'ultimo blocco del messaggio e la cifratura DES al penultimo passo
B. L'operazione di XOR fra l'output della cifratura DES dell'ultimo blocco del messaggio e il blocco precedente
C. L'operazione di XOR fra l'output della cifratura DES dell'ultimo blocco del messaggio e la chiave
D. L'operazione di XOR fra l'output della cifratura DES di tutti blocchi del messaggio

Answer: A
Section: I codici MAC

5. Quale dei seguenti non è un requisito dei codici MAC:
A. Deve essere computazionalmente impossibile che, dato il messaggio M e C(K,M), trovare un messaggio M' con C(K,M') = C(K,M)
B. Indicato con n il numero di bit di un codice MAC, la probabilità di collisione deve essere 1/2n
C. Indicato con n il numero di bit di un codice MAC, la probabilità di collisione deve essere 1/n
D. Dati due messaggi M e M' deve essere improbabile che C(k,M)= C(k,M')

Answer: C
Section: I codici MAC

6. Quale delle seguenti espressioni non rappresenta una funzione hash:

A. H(x)=h
B. G(k)=m
C. G(k,M)=h
D. G(h)=k

Answer: C
Section: Le funzioni hash

7. Nel caso di funzione hash basata sullo XOR di 4 blocchi di messaggio, ciascuno da 3 bit, si ha che:
A. L'hash è costituto da 3 bit
B. L'hash è costituto da 4 bit
C. L'hash è costituto da 12 bit
D. L'hash è costituto da 7 bit

Answer: A
Section: Le funzioni hash

8. Nel caso di funzione hash basata sullo XOR di blocchi di messaggio da 3 bit ciascuno, se un attaccante ha intercettato un hash H=010 quale dei seguenti falsi messaggi M' (da due blocchi) può inviare affinché M' sia accettato come valido rispetto a tale hash H:
A. M=[111; 000]
B. M=[111; 110]
C. M=[111; 101]
D. M=[101; 001]

Answer: C
Section: Le funzioni hash

9. Nel caso di 'attacco a compleanno' nei confronti di un codice hash a 48 bit, l'attaccante deve generare un numero di messaggi fraudolenti F pari a:
A. F=296
B. F=216
C. F=224
D. F=248

Answer: C
Section: Attacco a compleanno

10. Il 'paradosso del compleanno' stabilisce che:
A. Esiste una probabilità del 50% che in un gruppo di circa 23 persone ve ne siano due coetanee
B. Esiste una probabilità del 50% che in un gruppo di circa 23 persone ve ne siano due nate lo stesso giorno
C. Esiste una probabilità del 50% che in un gruppo di circa 50 persone ve ne siano due nate lo stesso giorno
D. Esiste una probabilità del 23% che in un gruppo di circa 50 persone ve ne siano due nate lo stesso giorno

Answer: B
Section: Attacco a compleanno

Id Lezione 32: L'algoritmo SHA-512

1. La struttura di base di una funzione hash come SHA-512 è costituita da:
A. L'applicazione ripetuta in cascata di diverse funzioni di compressione
B. L'applicazione ripetuta in cascata di una stessa funzione di compressione
C. L'applicazione ripetuta in parallelo di una stessa funzione di compressione
D. L'applicazione di una stessa funzione di compressione

Answer: B
Section: Lâ€™algoritmo SHA

2. Negli algoritmi hash di tipologia SHA, il numero delle fasi è dell'ordine di:
A. Circa 10
B. Circa 20
C. Circa 100
D. Circa 1000

Answer: C
Section: Lâ€™algoritmo SHA

3. Negli algoritmi hash di tipologia SHA, esiste un limite sulla lunghezza del messsaggio in ingresso:
A. No non esiste
B. Sì, devono essere multipli di 1024
C. Sì, devono essere multipli di 512
D. Sì, devono essere minori di 264 o 2128 dipende dalle versioni

Answer: D
Section: Lâ€™algoritmo SHA

4. L'algoritmo SHA-512 prende in input:
A. Blocchi di messaggio di 1024 bit
B. Blocchi di messaggio di 512 bit
C. Blocchi di messaggio di 256 bit
D. Blocchi di messaggio di dimensione variabili

Answer: A
Section: Lâ€™algoritmo SHA-512

5. L'algoritmo SHA-512 prevede di usare dei bit di riempimento per adattare:
A. La lunghezza del messaggio ad un numero di blocchi multiplo di 512
B. La lunghezza del messaggio ad un numero di blocchi multiplo di 1024
C. Il numero di blocchi da elaborare
D. La lunghezza del digest di output

Answer: B
Section: Lâ€™algoritmo SHA-512

6. L'algoritmo SHA-512 utilizza un buffer a 8 registri che serve per:
A. Appoggiare l'elaborazione di ogni fase
B. Solo per l'inizializzazione
C. Memorizzare le costanti

D. Il digest di uscita

Answer: A
Section: Lâ€™algoritmo SHA-512

7. Nell'algoritmo SHA-512 il digest di uscita è ottenuto:
A. Dopo aver eseguito l'elaborazione del modulo F ed effettuato la somma con l'output allo stadio precedente, per tutti gli N blocchi del messaggio
B. Dopo aver calcolato le 80 fasi
C. Dopo aver eseguito l'elaborazione del modulo F
D. Dopo aver eseguito l'elaborazione del modulo F ed effettuato la somma con l'input allo stadio precedente, per tutti gli N blocchi del messaggio

Answer: A
Section: Lâ€™algoritmo SHA-512

8. Nell'algoritmo SHA-512, le 80 word sono generate a partire da:
A. Sono fissate
B. Dal messaggio
C. Da un blocco del messaggio
D. Dal digest del blocco precedente

Answer: C
Section: Lâ€™algoritmo SHA-512

9. Quale affermazione sulle funzioni di fase interne al modulo F è falsa:
A. Sono in numero di 80
B. Prendono in input il buffer dei registri
C. Producono in output il buffer dei registri
D. Prendono in input il buffer dei registri, la word di fase e la costante di fase

Answer: B
Section: La funzione di fase di SHA-512

10. Le funzioni di fase interne al modulo F eseguono sostanzialmente:
A. Operazioni logiche
B. Operazioni AND e XOR
C. Permutazioni
D. Operazioni logiche, shift e somme modulari

Answer: D
Section: La funzione di fase di SHA-512

Id Lezione 33: Gli algoritmi HMAC e CMAC

1. L'algoritmo HMAC è:
A. Un algoritmo MAC basato su una funzione hash
B. Un algoritmo hash basato su una funzione di crittografia
C. Un algoritmo MAC basato su una funzione di crittografia
D. Un algoritmo MAC non basato su una funzione hash

Answer: A
Section: Caratteristiche dellâ€™algoritmo HMAC

2. Quali di queste affermazioni è vera per l'algoritmo HMAC:
A. Non è utilizzato per la sicurezza IP
B. La sicurezza di HMAC dipende direttamente dalla sicurezza della funzione di hash
C. La sicurezza di HMAC non dipende direttamente dalla sicurezza della funzione di hash
D. La struttura di HMAC degrada le performance delle funzioni hash utilizzate

Answer: B
Section: Caratteristiche dellâ€™algoritmo HMAC

3. Nell'algoritmo HMAC, i valori ipad e opad servono per:
A. Invertire lo stato dei bit della chiave
B. Invertire lo stato di metà dei bit della chiave
C. Mettere a 1 lo stato dei bit della chiave
D. Mettere a 0 lo stato dei bit della chiave

Answer: B
Section: Funzionamento dellâ€™algoritmo HMAC

4. Nell'algoritmo HMAC, la funzione di hash viene utilizzata:
A. 1 volta
B. 2 volte con vettore di inizializzazione uguale
C. 2 volte con vettore di inizializzazione diverso
D. 3 volte

Answer: B
Section: Funzionamento dellâ€™algoritmo HMAC

5. Nell'algoritmo HMAC, la chiave K+ viene ricavata a partire dalla chiave K:
A. Attraverso un'operazione di riempimento a sinistra con una serie di 0 fino ad avere lunghezza uguale a quello del blocco
B. Attraverso un'operazione di riempimento a sinistra con una serie di 1 fino ad avere lunghezza uguale a quello del blocco
C. Attraverso un'operazione di troncamento pari alla lunghezza del blocco
D. Attraverso un'operazione di XOR con il valore ipad oppure opad

Answer: A
Section: Funzionamento dellâ€™algoritmo HMAC

6. Nell'algoritmo HMAC, la chiave K+ viene usata:
A. Direttamente come input per la funzione di hash

B. Non viene usata
C. Come input per lo XOR con il messaggio
D. Integrata nel messaggo come input per la funzione di hash

Answer: D
Section: Funzionamento dellâ€™algoritmo HMAC

7. Nell'algoritmo HMAC, l'uscita del primo hash viene:
A. Non viene estesa
B. Estesa da n (lunghezza del digest) a b bit (lunghezza del blocco)
C. Troncata da n (lunghezza del digest) a b bit (lunghezza del blocco)
D. Estesa da n (lunghezza del digest) a 1024 bit

Answer: B
Section: Funzionamento dellâ€™algoritmo HMAC

8. Nell'algoritmo HMAC, l'input del primo hash è costituto da:
A. L blocchi
B. (L-1) blocchi
C. (L+1) blocchi
D. (L+b) blocchi

Answer: C
Section: Funzionamento dellâ€™algoritmo HMAC

9. I codici MAC basati su algoritmi di crittografia e cifratura a blocchi possono superare le loro debolezze in termini di sicurezza tramite:
A. Aumentando il numero di crittografie effettuate
B. L'introduzione di una doppia chiave generata a partire da una singola
C. L'introduzione di due chiavi diverse
D. Cambiando algoritmo crittografico

Answer: B
Section: Lâ€™algoritmo CMAC

10. L'algortimo CMAC usa come cifratura:
A. DES e AES
B. DES o AES
C. Solo DES
D. RSA

Answer: B
Section: Lâ€™algoritmo CMAC

Id Lezione 34: I certificati X.509

1. Trial di queste definizioni meglio definisce X.509:
A. Definisce la tipologia di crittografia pubblica da usare con i certificati
B. Definisce il formato dei certificati
C. Rappresenta un framework per servizi di autenticazione basato sull'uso di un repository e di certificati
D. Rappresenta un framework per servizi di crittografia pubblica basato sull'uso di un repository e di certificati

Answer: C
Section: Introduzione a X.509

2. Il certificato X.509 contiene:
A. Le chiavi privata e pubblica del possessore del certificato
B. La chiave pubblica del possessore del certificato
C. La chiave privata del possessore del certificato
D. La chiave pubblica della CA

Answer: B
Section: Introduzione a X.509

3. I certificati X.509 sono creati da:
A. Dall'Internet Service Provider
B. Dall'autorità che rilascia la CRL
C. Dall'utente stesso
D. Dall'autorità di certificazione

Answer: D
Section: Introduzione a X.509

4. In un certificato X.509, esistono sostanzialmente due parti:
A. La parte non firmata e la parte firmata dalla CA
B. La parte pubblica e la parte privata
C. La parte non firmata e la parte firmata dal possessore del certificato
D. La parte non firmata e la parte per la chiave pubblica

Answer: A
Section: Introduzione a X.509

5. Quali dei seguenti campi non fa parte del formato di un certificato X.509:
A. Numero seriale del certificato
B. Nome dell'emettitore
C. Chiave privata
D. Periodo di validità

Answer: C
Section: Formato certificato X.509

6. Nel formato del certificato X.509, il campo "periodo di validità" contiene:
A. Non esiste tale campo
B. La data di inizio della validità
C. La data di fine della validità

D. La data di inizio e fine della validità

Answer: D
Section: Formato certificato X.509

7. Se i certificati X.509 sono emessi da CA diverse accade che:
A. Gli utenti non possono comunicare
B. Non ci sono problemi le CA sono autenticate fra di loro
C. Gli utenti possono comunicare ma devono inviare i loro messaggi alle rispettive CA
D. Gli utenti possono comunicare ma devono inviare i loro messaggi ad una delle due CA

Answer: B
Section: Gestione certificati X.509

8. In quali casi un certificato X.509 non finisce in CRL (Certificate Revocation List):
A. Certificato scaduto
B. La chiave privata dell'utente è stata violata
C. L'utente non è più certificato da quella CA
D. Il certificato è stato violato

Answer: A
Section: Gestione certificati X.509

9. Nella CRL dei certificati X.509 quale dei seguenti campi non è presente:
A. La data di creazione della lista
B. La data del prossimo aggiornamento della lista
C. Il nome dell'autorità che ha emesso la CRL
D. La data in cui il certificato sarà di nuovo valido

Answer: D
Section: Gestione certificati X.509

10. Nell'infrastruttura PKIX per X.509, quale delle seguenti entità può non essere presente:
A. L'autorità di certificazione
B. L'utente finale
C. Il repository dei certificati
D. L'emettitore della CRL

Answer: D
Section: Gestione certificati X.509

Id Lezione 35: IPSec e il protocollo ESP

1. In IPSec, con il protocollo ESP si può realizzare:
A. Il servizio di autenticazione e opzionalmente il servizio di segretezza
B. Il servizio di segretezza e opzionalmente il servizio di autenticazione
C. Solo il servizio di segretezza
D. Il servizio di autenticazione

Answer: B
Section: Encapsulating Security Payload (ESP)

2. In IPSec, il protocollo ESP, diversamente da AH, garantisce:
A. La modalità tunnel
B. L'accesso da remoto
C. La segretezza
D. L'autenticazione

Answer: C
Section: Encapsulating Security Payload (ESP)

3. In IPSec, nel protocollo ESP, il campo Authentication Data è generato:
A. Tramite un codice MAC
B. Tramite un hash
C. Tramite cifratura RSA
D. Tramite un'operazione di XOR sui campi precedenti

Answer: A
Section: Encapsulating Security Payload (ESP)

4. In IPSec, nel protocollo ESP, il campo Padding serve fondamentalmente a:
A. Allineare le word dei campi nel pacchetto ESP
B. Si tratta di un campo opzionale
C. Adattare il campo Payload Data alle esigenze di lunghezza per la cifratura
D. Adattare il campo Payload Data alle esigenze di lunghezza per il calcolo del codice MAC

Answer: C
Section: Encapsulating Security Payload (ESP)

5. In IPSec, nel protocollo ESP in modalità trasporto, l'intestazione ESP si trova:
A. Prima della nuova intestazione IP
B. Dopo l'intestazione IP originaria
C. Prima dell'intestazione IP originaria
D. Dopo la nuova intestazione IP

Answer: B
Section: Encapsulating Security Payload (ESP)

6. In IPSec, esiste la necessità di impiegare combinazioni di SA per:
A. Non esiste una necessità
B. Implementare servizi di sicurezza diversi
C. Modificare i servizi di sicurezza in essere

D. Implementare più volte lo stesso servizio di sicurezza

Answer: B
Section: Combinazioni di associazioni di sicurezza

7. Nel caso di accesso host da remoto verso un server posto all'interno di una rete aziendale, quale di queste combinazione di SA appare più adatta:
A. Una SA di tipo trasporto
B. Una SA di tipo trasporto fra host e gateway della rete con una o due SA fra gateway e server
C. Una SA di tipo tunnel fra host e gateway della rete con una o due SA fra gateway e server
D. Una SA di tipo tunnel fra host e gateway della rete con una o due SA fra host e server

Answer: D
Section: Combinazioni di associazioni di sicurezza

8. In IPSec la gestione delle chiavi si basa fondamentalmente su:
A. Protocolli Oakley e ISAKMP
B. Diffie-Hellman
C. Protocollo Oakley
D. Protocollo ISAKMP

Answer: A
Section: Gestione delle chiavi

9. In IPSec, il protocollo Oakley permette di difendersi dagli attacchi replay tramite:
A. Cifratura RSA
B. L'uso di nonce
C. Modalità tunnel
D. Non permette di difendersi da attacchi replay

Answer: B
Section: Gestione delle chiavi

10. In IPSec, quali delle seguenti affermazioni è falsa nel protocollo ISAKMP:
A. ISAKMP prevede vari tipi di payload
B. ISAKMP prevede un'intestazione generica per i vari tipi di payload
C. ISAKMP non prevede un'intestazione ISAKMP ma solo un'intestazione generica
D. ISAKMP prevede un'intestazione ISAKMP e un'intestazione generica

Answer: C
Section: Gestione delle chiavi

Id Lezione 36: IPSec

1. Il protocollo IPSec consente di:
A. Bloccare tutti gli attacchi
B. Impedire il monitoraggio non autorizzato del traffico
C. Impedire l'accesso da remoto su una rete aziendale
D. Impedire il trasferimento di file da remoto su una rete aziendale

Answer: B
Section: Panoramica sulla sicurezza IP

2. Mediante il protocollo IPSec si può:
A. Crittografare e/o autenticare il traffico a livello IP
B. Distribuire chiavi crittografiche
C. Firmare documenti
D. Crittografare e/o autenticare il traffico a livello applicazione

Answer: A
Section: Panoramica sulla sicurezza IP

3. Il protocollo IPSec si basa sull'uso di extension header che:
A. Modificano l'intestazione IP
B. Precedono l'intestazione IP
C. Seguono l'intestazione IP
D. Cancellano l'intestazione IP

Answer: C
Section: Architettura e servizi IPSec

4. In IPSec, gli extension header possono identificare i protocolli:
A. AH o ESP
B. Solo AH
C. Solo ESP
D. Non identificano nessun protocollo

Answer: A
Section: Architettura e servizi IPSec

5. In IPSec, quale dei seguenti protocolli fornisce crittografia e autenticazione combinata:
A. Authentication Header
B. Encapsulated Security Payload
C. Encapsulated Security Payload e Authentication Header
D. Nessun protocollo

Answer: B
Section: Architettura e servizi IPSec

6. In IPSec, quale dei protocolli garantisce un set completo di servizi di sicurezza:
A. AH
B. ESP
C. ESP con l'opzione di autenticazione

D. Nessuno dei protocolli

Answer: C
Section: Architettura e servizi IPSec

7. In IPSec per Associazione di Sicurezza si intende:
A. Una relazione bidirezionale fra un mittente e un destinatario riguardante i servizi di sicurezza
B. Una relazione monodirezionale fra un mittente e un destinatario riguardante i servizi di sicurezza
C. Un servizio di sicurezza
D. Una relazione monodirezionale fra un mittente e un destinatario per lo scambio delle chiavi di cifratura

Answer: B
Section: Architettura e servizi IPSec

8. In IPSec, nella modalità tunnel, si fornisce protezione a:
A. L'intestazione IP
B. Il payload IP
C. L'intero pacchetto IP
D. Ad alcune parti dell'intestazione

Answer: C
Section: Architettura e servizi IPSec

9. In IPSec, il campo Sequence Number nell'Authetication Header serve a:
A. Inserire un valore casuale
B. Soltanto a numerare i pacchetti IP
C. Impedire attacchi replay
D. A tenere conto dei pacchetti IP passati

Answer: C
Section: Authentication Header (AH)

10. In IPSec, nel protocollo AH, la finestra anti-replay consente di:
A. Scartare i pacchetti non validi
B. Scartare i pacchetti con valore a sinistra della finestra anche se validi
C. Scartare i pacchetti con valore a sinistra della finestra se non validi
D. Scartare i pacchetti con valore a destra della finestra anche se validi

Answer: B
Section: Authentication Header (AH)

Id Lezione 37: Il protocollo SSL

1. Il protocollo SSL, nell'ambito dello stack dei protocolli TCP/IP, opera:
A. A livello IP
B. Sotto al livello TCP
C. Sopra al livello TCP
D. Allo stesso livello di IPSec

Answer: C
Section: Lâ€™architettura SSL

2. Il protocollo SSL è costituito da dei sotto-protocolli con le seguenti caratteristiche:
A. Due protocolli allo stesso livello
B. Un protocollo di base e tre protocolli a livello superirore
C. Due protocolli a differenti livelli
D. Un protocollo di base e uno a livello superiore

Answer: B
Section: Lâ€™architettura SSL

3. Una connessione SSL presenta le seguenti caratteristiche:
A. Può prevedere più servizi
B. Può essere stabilita all'interno di più sessioni
C. Viene stabilita all'interno di una singola sessione
D. Non condivide parametri di sicurezza con altre connessioni

Answer: C
Section: Lâ€™architettura SSL

4. In SSL, il protocollo SSL Record fornisce due servizi:
A. Un servizio di integrità e un servizio di segretezza
B. Un servizio di integrità e un servizio di hash
C. Un servizio di cifratura simmetrica e uno di cifratura asimmetrica
D. Un servizio di firma digitale e di anonimato

Answer: A
Section: SSL Record Protocol

5. Nel protocollo SSL Record, il servizio di integrità del messaggio è realizzato mediante:
A. Hash
B. Codice MAC
C. RSA
D. Cifratura simmetrica

Answer: B
Section: SSL Record Protocol

6. Nel protocollo SSL Record, la cifratura si applica a:
A. Al testo in chiaro/compresso, al codice MAC e all'intestazione
B. Al testo compresso
C. Al testo in chiaro

D. Al testo in chiaro/compresso e al codice MAC

Answer: D
Section: SSL Record Protocol

7. In SSL, il protocollo Change Cipher Spec specifica:
A. Di effettuare la decifratura
B. Di non effettuare la cifratura
C. Di cambiare la tipologia di cifratura
D. Di mantenere la tipologia di cifratura in uso

Answer: C
Section: I protocolli SSL Change Cipher Spec e Alert

8. In SSL, il protocollo Alert specifica:
A. Il livello di severità dell'alert e la sua tipologia
B. Il livello di severità dell'alert
C. Invia un alert
D. La tipologia di alert

Answer: A
Section: I protocolli SSL Change Cipher Spec e Alert

9. In SSL, il protocollo Handshake serve a:
A. Autenticazione del client
B. Autenticazione vicendevole del server e del client
C. Autenticazione del server
D. Inviare il codice MAC

Answer: B
Section: Il protocollo SSL Handshake

10. In SSL, quale delle seguenti non è una fase del protocollo Handshake :
A. Autenticazione del server e scambio delle chiavi
B. Inizializzazione delle funzionalità di sicurezza
C. Autenticazione del client e scambio delle chiavi
D. Autenticazione del client presso la CA

Answer: D
Section: Il protocollo SSL Handshake

Id Lezione 38: I protocolli TLS e HTTPS

1. Il protocollo TLS si presenta rispetto a SSL:
A. Identico
B. TLS è un'evoluzione di SSL
C. SSL è un'evoluzione di TLS
D. SSL è un sottoprotocollo di TLS

Answer: B
Section: Il protocollo TLS: introduzione

2. Quale delle seguenti non è una differenza fra SSL e TLS:
A. Usano diversi codici MAC
B. TLS usa una funzione di espansione dei valori segreti
C. TLS supporta codici di allarme addizionali
D. SSL si appoggia sul livello TCP mentre TLS sul livello IP

Answer: D
Section: Il protocollo TLS: introduzione

3. Nel protocollo TLS è prevista un'operazione di padding del tipo:
A. Tale da ottenere una lunghezza totale multipla della dimensione dell'intestazione
B. Tale da ottenere una lunghezza totale multipla della dimensione del blocco
C. Tale da ottenere un numero di blocchi multiplo di 128
D. Tale da ottenere la lunghezza totale minima di multipli della dimensione del blocco

Answer: B
Section: Il protocollo TLS: introduzione

4. Nel protocollo TLS, la funzione pseudo-random ha l'obiettivo di:
A. Generare numeri pseudo-casuali
B. Comprimere i valori segreti in una serie di blocchi di dati sicuri
C. Espandere i valori segreti in una serie di blocchi di dati sicuri
D. Generare un codice MAC

Answer: C
Section: Il protocollo TLS: la funzione pseudo-random

5. Nel protocollo TLS, la funzione pseudo-random può essere:
A. Iterata più volte per ottenere il numero di dati necessario
B. Iterata due volte
C. Iterata ma solo per un numero di volte definito dal protocollo stesso
D. Non può essere iterata

Answer: A
Section: Il protocollo TLS: la funzione pseudo-random

6. Nel protocollo TLS, la funzione pseudo-random ad ogni iterazione esegue la seguente operazione:
A. HMAC(secret, HASH || seed)
B. HMAC(secret, A(i+1))
C. HMAC(secret, A(i-1))

D. HMAC(secret, A(i-1) || seed)

Answer: D
Section: Il protocollo TLS: la funzione pseudo-random

7. Nel protocollo TLS, la funzione pseudo-random prende in ingresso:
A. Una chiave
B. Un valore segreto e un valore seed
C. Due valori segreti e un valore seed
D. Due chiavi, di cui una generata dall'altra

Answer: B
Section: Il protocollo TLS: la funzione pseudo-random

8. Il protocollo HTTPS è la combinazione di:
A. TLS e SSl
B. TLS(SSL) e FTP
C. TLS(SSL) e HTTP ma solo per casi specifici
D. TLS(SSL) e HTTP

Answer: D
Section: Il protocollo HTTPS

9. Nel protocollo HTTPS non vengono cifrati:
A. L'URL della risorsa richiesta
B. I contenuti della risorsa
C. I contenuti dell'header HTTP
D. L'intestazione IP

Answer: D
Section: Il protocollo HTTPS

10. Le porte utilizzate da HTTP e HTTPS sono rispettivamente:
A. 25 e 443
B. 80 e 25
C. 80 e 443
D. 443 e 80

Answer: C
Section: Il protocollo HTTPS

Id Lezione 39: Multimedia forensics

1. Il Digital Forensics è:
A. Una branca della scienza forense che estrae prove digitali dall'analisi del traffico di rete
B. Una branca della scienza forense che analizza immagini digitali
C. Una branca della scienza forense che analizza computer e dispositivi digitali
D. Una branca della scienza forense che analizza prove digitali recuperate da sorgenti digitali

Answer: D
Section: Digital forensics

2. La Mobile Device Forensics si occupa di:
A. Recuperare prove digitali da un hard disk
B. Recuperare prove digitali da dispositivi mobili
C. Intercettare conversazioni telefoniche
D. Intercettare un dispositivo mobile

Answer: B
Section: Digital forensics

3. La Network Forensics si occupa di:
A. Monitorare e analizzare il traffico di rete fra computer
B. Impedire l'accesso a un sistema
C. Impedire la diffusione di malware in rete
D. Monitorare e analizzare il traffico di fra due computer

Answer: A
Section: Digital forensics

4. Il Multimedia Forensics è un settore specifico del:
A. Forensics
B. Digital Forensics
C. Computer Forensics
D. Image Forensics

Answer: B
Section: Multimedia forensics: concetti base

5. Il Multimedia Forensics analizza:
A. Hard disk
B. Contenuti multimediali
C. Smartphone
D. Chiavi USB e tablet

Answer: B
Section: Multimedia forensics: concetti base

6. Il principio che sta alla base del MMForensics è:
A. Tutti i documenti multimediali portano con sé delle tracce
B. La creazione di un contenuto multimediale contiene una traccia
C. Ogni elaborazione effettuata su un documento multimediale ne altera i metadati

D. Ogni elaborazione effettuata su un documento multimediale lascia una traccia

Answer: D
Section: Multimedia forensics: concetti base

7. Nell'analisi di un contenuto multimediale, le tecniche di MM Forensics di solito dispongono di:
A. Un contenuto di riferimento
B. Nessun contenuto di riferimento
C. Del contenuto originale
D. Della fotocamera

Answer: B
Section: Multimedia forensics: concetti base

8. Le due macro-aree del MM Forensics riguardano:
A. Identificazione della sorgente di acquisizione e analisi dell'autenticità di tale sorgente
B. Identificazione della qualità e dell'autenticità di un contenuto
C. Identificazione della sorgente di acquisizione e analisi dell'autenticità di un contenuto
D. Analisi dell'autenticità di un contenuto e recupero dell'originale

Answer: C
Section: Multimedia forensics: concetti base

9. Esistono tecniche di MM Forensics che permettono di:
A. Determinare la sorgente di acquisizione che ha generato un determinato documento multimediale
B. Determinare la sorgente di acquisizione di un determinato documento multimediale ma non se in formato compresso
C. Determinare l'utente che ha acquisito un determinato contenuto multimediale
D. Determinare informazioni sugli utenti che sono in possesso di un determinato contenuto multimediale

Answer: A
Section: Identificazione della sorgente e integrità

10. Esistono tecniche di MM Forensics che consentono di determinare se un'immagine digitale è:
A. Contraffatta e di localizzare l'eventuale alterazione
B. Contraffatta ma solo in presenza dell'originale
C. Contraffatta ma solo se di alta qualità
D. Autentica ma solo tramite un'operazione di confronto

Answer: A
Section: Identificazione della sorgente e integrità

Id Lezione 40: MM-forensics: identificazione della sorgente

1. Esistono tecniche di MM Forensics che permettono di stabilire se:
A. Un'immagine proviene da una fotocamera o da uno scanner
B. Un'immagine proviene da una fotocamera o da una chiave USB
C. Un'immagine proviene da una fotocamera ma non è vero per i video
D. Un video proviene da una fotocamera ma non è vero per le immagini statiche

Answer: A
Section: Identificazione del dispositivo

2. Le tecniche di MM Forensics non consentono di stabilire se:
A. Un'immagine è stata acquisita da una certo modello di fotocamera
B. Un'immagine è stata acquisita da una certa marca di fotocamera
C. Un'immagine è stata acquisita da un certo dispositivo di fotocamera
D. Un'immagine è stata acquisita dal proprietario di un certo dispositivo

Answer: D
Section: Identificazione del dispositivo

3. Quali di questi processi o sistemi lascia una traccia sull'immagine durante la fase di acquisizione:
A. Il sensore ma non il sistema ottico
B. Il sensore e il processing interno alla fotocamera
C. Il sensore ma solo a certe risoluzioni
D. Il sensore ma dipende dal tipo di immagine

Answer: B
Section: Il processo di acquisizione

4. A cosa è dovuta la traccia relativa alla distorsione della lente:
A. Alla distorsione radiale indotta dal fatto che la lente non è ideale
B. Alla successiva compressione JPEG
C. Alla distorsione radiale indotta dal filtro ottico
D. Alla distorsione radiale indotta dal CFA

Answer: A
Section: Il processo di acquisizione

5. Il CFA serve a:
A. Ad unire le tre componenti di colore
B. A interploare le tre componenti di colore
C. Far passare le tre componenti di colore
D. Filtrare le componenti di colore

Answer: D
Section: Il processo di acquisizione

6. Cosa si ntende con il termine "demosaicking":
A. Un'operazione di esaltazione di valori di colore
B. Un'operazione di eliminazione di valori di colore
C. Un'operazione di generazione di valori di colore

D. Un'operazione di combinazione di valori di colore

Answer: C
Section: Il processo di acquisizione

7. Il rumore PRNU è generato da:
A. Il rumore di acquisizione
B. Una risposta differente dei CCD all'intensità di luce
C. Dal malfunzionamento dei CCD rispetto all'intensità di luce
D. Dal deterioramento nel tempo dei CCD

Answer: B
Section: Fingerprint e PRNU

8. Il rumore PRNU presenta le seguenti caratteristiche:
A. Moltiplicativo e sistematico
B. Moltiplicativo e dipendente dalla temperatura
C. Moltiplicativo e dipendente dal tempo
D. Sistematico e additivo

Answer: A
Section: Fingerprint e PRNU

9. Il fingerprint di una fotocamera si ottiene:
A. Attraverso un'operazione di stima estraendo i PRNU da un'immagine scattata dalla fotocamera stessa
B. Attraverso un'operazione di filtraggio del PRNU
C. Attraverso un'operazione di stima estraendo i PRNU da alcune immagini scattate dalla fotocamera stessa
D. Attraverso un'operazione di stima estraendo i PRNU da alcune immagini

Answer: C
Section: Fingerprint e PRNU

10. Esistono tecniche di MM Forensics che consentono di determinare se un'immagine:
A. Proviene da un social network ma non risalire alle condivisioni
B. Proviene da un social network ed eventualmente risalire alle condivisioni
C. Proviene da un social network ma se non è stata ricompressa JPEG
D. Proviene da un social network ma se non è stata modificata dal social network

Answer: B
Section: Identificazione origine

Id Lezione 41: MM-forensics: rilevazione di fake

1. Le tecniche di MM Forensics permettono di stabilire se un contenuto multimediale sia o meno un falso basandosi su:
A. I metadati associati ad un file multimediale
B. L'analisi visiva di un'immagine o di un video
C. L'analisi di caratteristiche intrinseche di un contenuto multimediale
D. Il tipo di formato

Answer: C
Section: Tecniche per la rilevazione di manipolazioni

2. Le tecniche di MM Forensics stabiliscono se un'immagine è reale o è un fake ricorrendo all'uso di:
A. Analisi del contrasto dell'immagine
B. Analisi di elementi fisici o di descrittori relativi all'immagine
C. Analisi dei colori relativi all'immagine
D. Solo analizzando le caratteristiche del formato JPEG

Answer: B
Section: Tecniche per la rilevazione di manipolazioni

3. Alcune tecniche di MM Forensics, per la rilevazione di immagini fake, basate sull'analisi degli elementi fisici presenti nell'immagine stessa, considerano:
A. L'inconsistenza della direzione di luce
B. L'inconsistenza della luminosità
C. L'inconsistenza del livello di grigio delle ombre
D. L'inconsistenza della forma delle ombre

Answer: A
Section: Tecniche basate sugli elementi fisici

4. Le tecniche di MM Forensics, basate sull'analisi delle traiettorie degli oggetti, sono utilizzate per:
A. Determinare se il formato di codifica di una sequenza video è stato manipolato
B. Determinare se un'immagine è manipolata
C. Non esistono tecniche di questo tipo
D. Determinare se una sequenza video è manipolata

Answer: D
Section: Tecniche basate sugli elementi fisici

5. Le tecniche di MM Forensics basate sui descrittori servono principalmente per individuare l'attacco di tipo:
A. Doppia compressione JPEG
B. Filtraggio mediano
C. Giustapposizione
D. Copy-move

Answer: D
Section: Tecniche basate sui descrittori

6. Nel MM Forensics, quali sono generalmente le fasi operative per la localizzazione in un'immagine di un attacco copy-move:

A. Calcolo dei descrittori, matching, clustering e localizzazione
B. Calcolo dei descrittori e localizzazione
C. Calcolo dei descrittori, clustering e localizzazione
D. Calcolo dei descrittori, filtraggio, clustering e localizzazione

Answer: A
Section: Tecniche basate sui descrittori

7. Le tecniche di MM Forensics, basate sull'analisi della doppia compressione JPEG, sono specifiche per individuare in un'immagine quale tipo di attacco:
A. Copy-move
B. Splicing
C. Filtraggio mediano
D. Equalizzazione dell'istogramma

Answer: B
Section: Tecniche basate sui formati

8. In MM Forensics, nel caso della tecnica JPEG Ghost, si procede calcolando successive differenze fra:
A. L'immagine da analizzare e le sue versioni filtrate a con differenti finestre di filtro
B. L'immagine da analizzare e la sua versione compressa due volte
C. L'immagine da analizzare e le sue versioni ricompresse a differenti fattori di qualità
D. Le varie versioni dell'immagine da analizzare ricompresse a differenti fattori di qualità

Answer: C
Section: Tecniche basate sui formati

9. Nel caso di uso di tecniche di MM Forensics in applicazioni per il cyberbullismo,si può riuscire a:
A. Rintracciare in rete la foto/video di un atto di bullismo
B. Determinare un collegamento tra il dispositivo di acquisizione di una foto/video di un atto di bullismo e la foto/video stesso
C. Determinare un collegamento diretto tra l'autore di una foto/video di un atto di bullismo e la foto/video stesso
D. Eviatre la condivisione in rete di una foto/video di un atto di bullismo

Answer: B
Section: Alcune cyber-applicazioni

10. Nel caso di attacchi di Adversarial Machine Learning, l'attaccante ha lo scopo di:
A. Indurre in errore il classificatore, basato su ML, attraverso la generazione di un'immagine compressa due volte
B. Inibire il classificatore, basato su ML, attraverso una serie di richieste
C. Indurre in errore il classificatore, basato su ML, attraverso una modifica dell'immagine
D. Indurre in errore il classificatore, basato su ML, mantenendo percettivamente minima la modifica apportata all'immagine di ingresso

Answer: D
Section: Alcune cyber-applicazioni

Id Lezione 42: Blockchain e Proof-of-Work

1. La Blockchain è:
A. Una tecnologia esclusiva per il trasferimento di denaro
B. Una tecnologia basata su Bitcoin
C. Una tecnologia che utilizza strumenti crittografici e DLT
D. Una tecnologia basata su criptovalute

Answer: C
Section: Introduzione

2. I vantaggi base offerti da Blockchain sono:
A. Trasferimenti di denaro più veloci ma con costi superiori
B. Transazioni quasi istantanee, senza intermediari e costi ridotti
C. Trasferimenti di denaro quasi istantanei e costi ridotti verso la banca
D. Zero commissioni bancarie

Answer: B
Section: Introduzione

3. Quali delle seguenti affermazioni su Blockchain è errata:
A. Ogni blocco della catena dipende dal precedente
B. Ogni blocco della catena contiene informazioni su delle transazioni
C. Ogni blocco della catena contiene informazioni su delle transazioni ma non si vedono le cifre coinvolte
D. Le identità dei soggetti coinvolti nelle transazioni non sono in chiaro

Answer: C
Section: La struttura della blockchain

4. Ogni blocco della Blockchain contiene:
A. Hash del blocco precedente e di quello attuale, le transazioni e anche l'hash di quello successivo
B. Hash del blocco precedente ma non di quello attuale
C. I dati relativi alle transazioni
D. Hash del blocco attuale

Answer: A
Section: La struttura della blockchain

5. Per generare l'hash di un blocco della Blockchain, i dati che vengono passati in input all'hash sono:
A. L'hash del blocco precedente e il nonce
B. I dati delle transazioni del blocco attuale, l'hash del blocco precedente e il nonce
C. I dati delle transazioni del blocco attuale e l'hash del blocco precedente
D. I dati delle transazioni del blocco attuale, l'hash del blocco precedente, il nonce del blocco precedente e di quello attuale

Answer: B
Section: La struttura della blockchain

6. In Blockchain, cosa rappresenta il nonce:
A. Un numero casuale
B. Il numero soluzione della PoW

C. La chiave dell'hash
D. L'uscita dell'hash

Answer: B
Section: La struttura della blockchain

7. In Blockchain, cos'è la Proof-of-Work:
A. Un problema di sicurezza
B. Un problema crittografico senza soluzione
C. Un problema crittografico computazionalmente semplice ma la cui verifica del risultato ottenuto è molto complessa
D. Un problema crittografico computazionalmente complesso ma la cui verifica del risultato ottenuto è molto semplice

Answer: D
Section: La Proof-of-Work (PoW)

8. In Blockchain, in cosa consiste la Proof-of-Work:
A. Trovare un nonce
B. Trovare un nonce tale che l'hash del nonce stesso e di altri dati produca un codice hash con caratteristiche specifiche
C. Trovare un nonce tale che l'hash di altri dati produca un codice hash con caratteristiche specifiche
D. Trovare un nonce le cui cifre iniziali siano degli 0

Answer: B
Section: La Proof-of-Work (PoW)

9. Se un attaccante modifica un dato di un blocco della Blockchain succede che:
A. Tutti i blocchi della Blockchain sono invalidati
B. Il blocco attuale e tutti quelli successivi della Blockchain sono invalidati
C. Cambiano solo gli hash del blocco attuale e del successivo
D. Cambiano i nonce del blocco attuale e del successivo

Answer: B
Section: La Proof-of-Work (PoW)

10. Un attaccante che modifica un blocco della Blockchain deve:
A. Un diverso nonce ma che cominci per 0
B. Usare lo stesso nonce ma un diverso hash valido
C. Ritrovare un nuovo nonce e conseguentemente un diverso hash valido
D. Ritrovare un nuovo nonce ma riprodurre lo stesso hash valido

Answer: C
Section: La Proof-of-Work (PoW)

Id Lezione 43: Blockchain e il Ledger Distribuito

1. In Blockchain, la sicurezza è data da:
A. La rete P2P e il Ledger distribuito
B. La rete P2P
C. IL Ledger distribuito
D. Il grande numero di nodi presenti nella rete P2P

Answer: A
Section: La rete P2P e il Ledger

2. In Blockchain, un attaccante che sia riuscito a ricalcolare una blockchain "modificata" è in grado di:
A. Alterare il Ledger distribuito inviando a tutti la nuova blockchain
B. Alterare il Ledger distribuito
C. Alterare il Ledger distribuito solo se guadagna il consenso della metà più uno dei nodi della rete P2P
D. Alterare il Ledger distribuito solo se guadagna il consenso di alcuni nodi della rete P2P

Answer: C
Section: La rete P2P e il Ledger

3. In Blockchain, ognuno dei nodi della rete P2P possiede:
A. Una versione del Ledger non pubblica
B. Una versione del Ledger
C. Una versione del Ledger sincronizzata
D. Una versione del Ledger e l'ultimo blocco

Answer: C
Section: La rete P2P e il Ledger

4. Il processo di "mining" consiste in:
A. Recuperare Bitcoin distribuiti nella rete P2P
B. Risolvere la PoW e ottenere Bitcoin
C. Aggiornare la blockchain
D. Aggiornare il Ledger distribuito

Answer: B
Section: Il processo di mining

5. I "miner" sono:
A. Nodi di attacco alla blockchain
B. Nodi della rete P2P
C. Nodi specifici della rete P2P che si occupano aggiornare il Ledger
D. Nodi specifici della rete P2P che si occupano di risolvere le PoW

Answer: D
Section: Il processo di mining

6. I "miner" svolgono il compito primario di:
A. Aggiungere un nuovo blocco alla blockchain
B. Risolvere un problema crittografico complesso
C. Verificare le soluzioni delle PoW

D. Aggiornarsi sulla rete P2P

Answer: B
Section: Il processo di mining

7. Una volta che un "miner" ha trovato la soluzione deve:
A. Aggiungere il nuovo blocco alla blockchain
B. Richiedere la ricompensa in BTC
C. Pubblicarla agli altri nodi
D. Pubblicarla nel Ledger

Answer: C
Section: Il processo di mining

8. In una transazione blockchain, i nodi della rete verificano:
A. La correttezza della transazione
B. La provenienza della richiesta
C. La PoW
D. L'hash del blocco

Answer: A
Section: Funzionamento delle transazioni

9. Se un "miner" che sta risolvendo una PoW viene battuto sul tempo da un altro deve:
A. Finire di risolvere la PoW
B. Controllare la soluzione trovata dall'altro
C. Riuscire a trovare la soluzione anche se in breve tempo
D. Disconnettrsi dalla rete P2P

Answer: B
Section: Funzionamento delle transazioni

10. Stando ai dati di Giugno 2019, la dimensione della blockchain di Bitcoin era dell'ordine di:
A. 100 MB
B. 1 GB
C. 100 GB
D. 1 TB

Answer: C
Section: Alcuni numeri su Bitcoin

Id Lezione 44: Comunicazioni anonime: i protocolli Crowds e Mix

1. Qual è il concetto che sta dietro la necessità di comunicazioni anonime:
A. Svolgere attività fraudolente
B. Proteggere i messaggi dei soggetti coinvolti
C. Proteggere le identità dei soggetti coinvolti
D. Accedere ad informazioni compromettenti

Answer: C
Section: Comunicazioni anonime

2. Quale delle seguenti affermazioni in merito alle comunicazioni anonime è corretta:
A. Effettuare la comunicazione con un proxy garantisce sempre l'anonimato del mittente
B. La crittografia non è sufficiente a garantire anonimato
C. Effettuare la comunicazione con un proxy garantisce sempre l'anonimato
D. La crittografia è sufficiente a garantire anonimato

Answer: B
Section: Comunicazioni anonime

3. L'idea base del protocollo Crowds è quella di:
A. Nascondere le comunicazioni di un utente facendole passare casualmente in un gruppo di utenti simili
B. Nascondere le comunicazioni di un utente facendole passare da un proxy
C. Nascondere le comunicazioni di un utente facendole passare sempre dagli stessi utenti del crowd
D. Annidare le comunicazioni secondo la tecnica di onion routing

Answer: A
Section: Il protocollo Crowds

4. Nel protocollo Crowds, la richiesta del mittente:
A. Segue un percorso non casuale
B. Passa da un solo jondo del crowd
C. Attraversa tutti i proxy jondo del crowd
D. Attraversa alcuni proxy jondo del crowd

Answer: D
Section: Il protocollo Crowds

5. Nel protocollo Crowds, un proxy jondo decide di inoltrare la richiesta ricevuta verso un altro jondo se:
A. La richiesta è già passata da un numero sufficiente di jondo
B. La richiesta contiene un'intestazione specifica
C. Il risultato del lancio di una moneta indica di inoltrare
D. Si è esaurito il numero di passaggi previsto

Answer: C
Section: Il protocollo Crowds

6. Nel protocollo Crowds, i collegamenti fra proxy jondo sono:
A. Cifrati con crittografia a chiave pubblica
B. Cifrati con crittografia a chiave simmetrica
C. Non cifrati

D. Cifrati con crittografia a chiave pubblica ma solo all'ingresso e all'uscita del crowd

Answer: A
Section: Il protocollo Crowds

7. Nel protocollo Mix, ogni proxy possiede:
A. Una coppia di chiavi pubblica/privata
B. Una chiave segreta
C. La chiave pubblica del proxy con cui deve comunicare
D. La chiave pubblica del mittente

Answer: A
Section: Il protocollo Mix

8. Nel protocollo Mix, il messaggio del mittente verso il destinatario è cifrato con:
A. Le chiavi private dei proxy da cui deve transitare
B. La chiave pubblica del primo proxy
C. Le chiavi pubbliche dei proxy da cui deve transitare
D. La chiave pubblica dell'ultimo proxy

Answer: C
Section: Il protocollo Mix

9. Nel protocollo Mix, il messaggio del mittente verso il destinatario è cifrato nel seguente ordine:
A. Non esiste un ordine definito
B. Prima la cifratura relativa all'ultimo proxy e poi le altre
C. Prima la cifratura relativa al primo proxy e poi le altre
D. Prima la cifratura relativa all'ultimo proxy e poi quella relativa al primo proxy

Answer: B
Section: Il protocollo Mix

10. Nel protocollo Mix, si implementa anche un'operazione di "mixing" che consiste nel:
A. Raccogliere richieste in un certo intervallo di tempo e mescolarle
B. Inviare traffico "dummy"
C. Raccogliere richieste in un certo intervallo di tempo e reinoltrarle con ritardi definiti
D. Raccogliere richieste in un certo intervallo di tempo e reinoltrarle in ordine casuale

Answer: D
Section: Il protocollo Mix

Id Lezione 45: Comunicazioni anonime: Tor e Deep Web

1. La rete Tor è basata su:
A. Il protocollo Crowd
B. Il protocollo MIX
C. Il protocollo SSL
D. Il protocollo Diffie-Hellman

Answer: B
Section: La rete Tor

2. Nella rete Tor, la lista dei Tor relay si ottiene da:
A. Un qualsiasi Tor relay
B. I Tor relay di guardia
C. Un directory server
D. Da una CA

Answer: C
Section: La rete Tor

3. Nella rete Tor, una volta instaurato, il percorso fra i Tor relay viene:
A. Mantenuto per sempre
B. Per un certo periodo di tempo
C. Fino a quando non viene individuato
D. Fino a quando non cade la connessione

Answer: B
Section: La rete Tor

4. Nella rete Tor, i Tor relay di guardia servono a:
A. Non hanno compiti particolari
B. Impedire ad un attaccante di connettersi alla rete Tor
C. Impedire ad un attaccante di diventare un relay del circuito
D. Impedire ad un attaccante di diventare il primo relay del circuito

Answer: D
Section: La rete Tor

5. Nella rete Tor, i "servizi nascosti" sono:
A. Servizi web a cui non si riesce ad accedere
B. Servizi di cui non è visibile l'indirizzo IP
C. Servizi web non legittimi
D. Servizi a cui si accede solo dopo una registrazione specifica

Answer: B
Section: Tor: servizi nascosti

6. Nell'accesso ai "servizi nascosti" della rete Tor, i punti di introduzione sono:
A. Punti di accesso alla rete Tor
B. Dei Tor relay su cui accedere ad un "servizio nascosto"
C. Dei Tor relay su cui il "servizio nascosto" espone il proprio servizio

D. Dei server di guardia

Answer: C
Section: Tor: servizi nascosti

7. Nell'accesso ai "servizi nascosti" della rete Tor, cosa rappresenta un relay di rendezvous:
A. Un Tor relay selezionato dall'utente per ricevere il servizio
B. Un Tor relay di guardia
C. Un relay scelto fra i punti di introduzione
D. Un Tor relay selezionato dal "servizio nascosto" per erogarvi il servizio

Answer: A
Section: Tor: servizi nascosti

8. Nell'accesso ai "servizi nascosti" della rete Tor, dove l'utente comunica il Tor relay di rendezvous:
A. Su più Tor relay
B. Su un qualsiasi Tor relay
C. Sul Tor relay di rendezvous
D. In uno dei punti di introduzione

Answer: D
Section: Tor: servizi nascosti

9. Quale delle seguenti affermazioni sul Deep Web è vera:
A. Nel Deep Web ci sono solo contenuti proibiti
B. Nel Deep Web ci sono pagine indicizzate
C. Nel Deep Web ci sono le pagine non indicizzate
D. Il Deep Web è solo una porzione ridotta del web

Answer: C
Section: Deep Web

10. Il Deep Web è accessibile tramite:
A. Un comune browser
B. La rete Tor
C. La cifratura asimmetrica
D. Un portale protetto

Answer: B
Section: Deep Web

Id Lezione 666: AUTOVALUTAZIONE

Q451. Un accesso residenziale ad Internet di tipo DSL (Digital Subscriber Line) utilizza:
A. La rete in fibra ottica fino all abitazione dell utente per trasmettere dati digitali convertiti in segnali ottici mediante un terminale ottico detto ONT (Optical Network Terminator)
B. La rete della televisione via cavo per trasmettere dati digitali convertiti mediante un cable modem
C. La rete satellitare della telefonia cellulare
D. La rete analogica telefonica per trasmettere dati digitali convertiti in formato analogico mediante un modem

Answer: D
Section: AUTOVALUTAZIONE

Q452. In una rete di calcolatori, il throughput medio end-to-end di una trasmissione di dati tra due sistemi periferici è una misura:
A. Del numero di errori che si verificano nella trasmissione client-server
B. Delle prestazioni del sistema periferico client
C. Delle prestazioni della rete
D. Delle prestazioni del sistema periferico server

Answer: C
Section: AUTOVALUTAZIONE

Q453. Una DoS provocata da un attacco alla vulnerabilità del sistema è:
A. Una interruzione del servizio causata dall'invio ad una applicazione vulnerabile o al Sistema Operativo in esecuzione sul server sotto attacco, di una sequenza di pacchetti opportunamente costruiti per determinare il blocco del servizio o anche lo spegnimento del server
B. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server
C. Una interruzione del servizio causata da una gran numero di connessioni TCP generate dall'attaccante e mantenute tutte aperte per ingorgare la capacità ricettiva del server
D. La diffusione in rete di copie dei file memorizzati su un computer

Answer: A
Section: AUTOVALUTAZIONE

Q454. Quale delle seguenti affermazioni è vera:
A. L'algoritmo di cifratura deve essere necessariamente segreto
B. L'attaccante non deve conoscere l'algoritmo di decifratura
C. La chiave deve restare segreta
D. L'attaccante non deve conoscere copie testo in chiaro/cifrato

Answer: C
Section: AUTOVALUTAZIONE

Q455. L'attacco "Testo in chiaro noto" prevede:
A. La conoscenza soltanto dell'algoritmo di cifratura
B. La disponibilità di più testi cifrati
C. La disponibilità di un solo testo cifrato
D. La disponibilità di più coppie di testo in chiaro e cifrato

Answer: D

Section: AUTOVALUTAZIONE

Q456. Conoscendo la seguente coppia testo in chiaro/testo cifrato BASE/AZRD secondo la cifratura di Giulio Cesare, determinare la chiave segreta K:
A. 1
B. 26
C. 25
D. 3

Answer: C
Section: AUTOVALUTAZIONE

Q457. Nella cifratura di Feistel cosa accade tra una fase e la successiva:
A. La parte REi viene sostituita nella parte LEi+1
B. La parte REi+1 viene sostituita nella parte LEi+1
C. La parte REi+1 viene sostituita nella parte LEi
D. La parte REi+1 viene permutata

Answer: A
Section: AUTOVALUTAZIONE

Q458. Nella cifratura di Feistel accade che:
A. Ogni fase usa la stessa sottochiave
B. La parte LEi va in XOR con F(REi, Ki+1)
C. La parte REi va in XOR con F(LEi, Ki+1)
D. La parte LEi va in XOR con REi

Answer: B
Section: AUTOVALUTAZIONE

Q459. Nella decifratura di Feistel si ha che:
A. Le sottochiavi sono in numero minore rispetto alla cifratura
B. Le sottochiavi si usano in ordine inverso
C. Le sottochiavi si usano nel medesimo ordine
D. Le sottochiavi si usano in ordine inverso e permutate

Answer: B
Section: AUTOVALUTAZIONE

Q460. Quale di queste affermazioni sulla nascita del DES non è corretta:
A. Deriva da un algoritmo di nome LUCIFER
B. Si basava sull'uso di strutture S-box
C. Si basava sull'uso di blocchi di Feistel
D. Usava una cifratura diversa dalla decifratura

Answer: D
Section: AUTOVALUTAZIONE

Q461. In ciascuna fase la parte Ri-1:
A. Viene inizialmente espansa a 56 bit
B. Non viene elaborata

C. Viene inizialmente espansa a 48 bit e permutata
D. Viene inizialmente espansa ma non permutata

Answer: C
Section: AUTOVALUTAZIONE

Q462. Nella generazione della chiave DES:
A. 8 bit dei 64 sono scartati casualmente
B. 8 bit dei 64 che si trovano nelle posizioni multiple di 8 sono scartati
C. Nessun bit viene scartato
D. I primi 8 bit sono scartati

Answer: B
Section: AUTOVALUTAZIONE

Q463. Nell'Attacco MitM si suppone di:
A. Conoscere una coppia (P, C) e una chiave
B. Conoscere almeno una chiave
C. Conoscere almeno una coppia (P, C)
D. Non conoscere niente

Answer: C
Section: AUTOVALUTAZIONE

Q464. Nella modalità Output Feedback cosa cambia rispetto a Cipher Feedback:
A. Nel registro a scorrimento vengono inseriti b bit che escono dalla cifratura al passo precedente e non quelli che escono dallo XOR con il testo in chiaro
B. Nel registro a scorrimento vengono inseriti s bit del testo in chiaro al passo precedente e non quelli che escono dallo XOR con il testo in chiaro
C. Nel registro a scorrimento vengono inseriti s bit che escono dalla cifratura al passo precedente e non quelli che escono dallo XOR con il testo in chiaro
D. Nel registro a scorrimento vengono inseriti s bit che escono dalla cifratura al passo precedente in XOR con la chiave e non quelli che escono dallo XOR con il testo in chiaro

Answer: C
Section: AUTOVALUTAZIONE

Q465. La cifratura end-to-end viene inserita a:
A. I livelli più bassi della gerarchia OSI
B. I livelli più alti della gerarchia OSI
C. Al livello "fisico" della gerarchia OSI
D. Al livello "collegamento" della gerarchia OSI

Answer: B
Section: AUTOVALUTAZIONE

Q466. La struttura di base di una funzione hash come SHA-512 è costituita da:
A. L'applicazione ripetuta in cascata di diverse funzioni di compressione
B. L'applicazione ripetuta in cascata di una stessa funzione di compressione
C. L'applicazione ripetuta in parallelo di una stessa funzione di compressione
D. L'applicazione di una stessa funzione di compressione

Answer: B
Section: AUTOVALUTAZIONE

Q467. Nell'algoritmo SHA-512, le 80 word sono generate a partire da:
A. Sono fissate
B. Dal messaggio
C. Da un blocco del messaggio
D. Dal digest del blocco precedente

Answer: C
Section: AUTOVALUTAZIONE

Q468. La fase di propagazione del virus coincide con:
A. L'avvio della sua azione dolosa
B. Lo svolgimento della sua azione dolosa
C. L'inserimento di copie di se stesso in altri programmi, dischi o memorie
D. La replica di file infetti

Answer: C
Section: AUTOVALUTAZIONE

Q469. Con il termine "virus polimorfico" si intende:
A. Un virus che attacca file di tipo diverso
B. Un virus che quando si replica modifica il suo aspetto e la sua tipologia di attacco
C. Un virus che quando si replica non modifica il suo aspetto pur eseguendo diversi tipi di attacco
D. Un virus che quando si replica modifica il suo aspetto ma esegue la stessa tipologia di attacco

Answer: D
Section: AUTOVALUTAZIONE

Q470. In Kerberos V4, la risposta dell'AS alla richiesta del client è:
A. Cifrata con cifratura simmetrica
B. Cifrata con cifratura asimmetrica
C. Non cifrata
D. Cifrata con cifratura simmetrica ma il client non può decifrarla

Answer: A
Section: AUTOVALUTAZIONE

Q471. In Kerberos V4, l'AutenticatoreC inviato dal client al TGS è cifrato con:
A. La chiave segreta del server TGS
B. La chiave Kc,tgs
C. La chiave pubblica del server TGS
D. La chiave privata del client

Answer: B
Section: AUTOVALUTAZIONE

Q472. I certificati X.509 sono creati da:
A. Dall'Internet Service Provider

B. Dall'autorità che rilascia la CRL
C. Dall'utente stesso
D. Dall'autorità di certificazione

Answer: D
Section: AUTOVALUTAZIONE

Q473. In IPSec, quali delle seguenti affermazioni è falsa nel protocollo ISAKMP:
A. ISAKMP prevede vari tipi di payload
B. ISAKMP prevede un'intestazione generica per i vari tipi di payload
C. ISAKMP non prevede un'intestazione ISAKMP ma solo un'intestazione generica
D. ISAKMP prevede un'intestazione ISAKMP e un'intestazione generica

Answer: C
Section: AUTOVALUTAZIONE

Q474. Nel protocollo TLS, la funzione pseudo-random ad ogni iterazione esegue la seguente operazione:
A. HMAC(secret, HASH || seed)
B. HMAC(secret, A(i+1))
C. HMAC(secret, A(i-1))
D. HMAC(secret, A(i-1) || seed)

Answer: D
Section: AUTOVALUTAZIONE

Q475. Nello standard SET l'integrità dei dati trasmessi è garantita attraverso:
A. Cifratura simmetrica DES
B. La firma digitale basata su RSA e i codici hash SHA-1
C. Cifratura simmetrica 3DES
D. La codifica hash SHA-1

Answer: B
Section: AUTOVALUTAZIONE

Q476. Nella fase di Authorization Request dello standard SET, il venditore invia al gateway di pagamento:
A. Nessuna chiave simmetrica
B. Una chiave simmetrica monouso diversa da quella inviatagli dal cliente
C. Una chiave simmetrica monouso uguale a quella inviatagli dal cliente
D. La propria chiave privata

Answer: B
Section: AUTOVALUTAZIONE

Q477. Quale di questi malware è specifico della posta elettronica:
A. Bomba logica
B. Worm
C. Virus
D. Spammer

Answer: D
Section: AUTOVALUTAZIONE

Q478. Le tecniche di MM Forensics, basate sull'analisi della doppia compressione JPEG, sono specifiche per individuare in un'immagine quale tipo di attacco:
A. Copy-move
B. Splicing
C. Filtraggio mediano
D. Equalizzazione dell'istogramma

Answer: B
Section: AUTOVALUTAZIONE

Q479. Nel protocollo Crowds, i collegamenti fra proxy jondo sono:
A. Cifrati con crittografia a chiave pubblica
B. Cifrati con crittografia a chiave simmetrica
C. Non cifrati
D. Cifrati con crittografia a chiave pubblica ma solo all'ingresso e all'uscita del crowd

Answer: A
Section: AUTOVALUTAZIONE

Q480. Nella rete Tor, una volta instaurato, il percorso fra i Tor relay viene:
A. Mantenuto per sempre
B. Per un certo periodo di tempo
C. Fino a quando non viene individuato
D. Fino a quando non cade la connessione

Answer: B
Section: AUTOVALUTAZIONE

Q481. Il vantaggio dell'uso dei sistemi di calcolo distribuito che impiegano calcolatori in rete, rispetto ai computer di grandi dimensionei, è dato da:
A. La tolleranza dei guasti, l'economicità dell'Hardware e del Software, la scalabilità che consente gradualità della crescita e flessibilità
B. La possibilità per i programmatori di comunicare tra loro attraverso la rete
C. La possibilità di risolvere un maggior numero di problemi
D. La possibilità di gestire dati di dimensione maggiore

Answer: A
Section: AUTOVALUTAZIONE

Q482. Nell'accesso a Internet mediante una LAN i dispositivi periferici sono collegati:
A. Mediante linee costituite da un doppino di rame intrecciato ad un DSLAM (Digital Subscriber Line Access Multiplexer) che è connesso a Internet tramite un router aziendale
B. Mediante linee costituite da un doppino di rame intrecciato ad un ONT (Optical Network Terminator) che è connesso a Internet tramite un router aziendale
C. Mediante linee costituite da un doppino di rame intrecciato ad uno switch Eternet che è connesso a Internet tramite un router aziendale
D. Mediante linee costituite da un doppino di rame intrecciato ad un OLT (Optical Line Terminator) che è connesso a Internet tramite un router aziendale

Answer: C

Section: AUTOVALUTAZIONE

Q483. In una trasmissione store and forward il router individua il collegamento in uscita su cui instradare il pacchetto mediante:

A. Informazioni memorizzate nel computer da cui parte la trasmissione del pacchetto

B. La tabella di inoltro che mette in corrispondenza l'indirizzo IP del pacchetto con i collegamenti di entrata del router

C. Informazioni memorizzate in un server del provider

D. La tabella di inoltro che mette in corrispondenza l'indirizzo IP del pacchetto con i collegamenti di uscita del router

Answer: D
Section: AUTOVALUTAZIONE

Q484. Il multi-homing consiste:

A. Nella connessione a Internet pagando il traffico ad un ISP regionale che a sua volta paga il traffico ad un fornitore di livello 1

B. Nella possibilità di connettersi affittando un collegamento ad alta velocità ad un gruppo di router che appartengono alla rete di un ISP e sono posizionati fisicamente vicini

C. Nella possibilità per tutti gli ISP di connettersi a due o più fornitori di livello superiore. Sono esclusi gli ISP di livello 1 che non pagano fornitori

D. In un collegamento tra due sistemi periferici che attraversa più ruter appartenenti a reti di ISP di livello gerarchico diverso

Answer: C
Section: AUTOVALUTAZIONE

Q485. Un IXP (Internet exchange Point) consiste:

A. Nel collegamento tra due sistemi periferici tramite un router nella rete di un ISP regionale

B. In un gruppo di router collocati fisicamente vicini che appartiene alla rete di un ISP fornitore. L'ISP fornitore che possiede un IXP offre ai propri ISP clienti la possibilità di collegare un loro router direttamente ad un router del IXP, mediante un collegamento ad alta velocità. Gli ISP di accesso che hanno come clienti gli utenti finali non posseggono IXP.

C. Nel pagamento ad un ISP di livello gerarchico superiore del traffico che passa attraverso un router

D. In un insieme di attrezzature e servizi che consentono ad ISP di ottimizzare i costi di una connessione di tipo peering tra le loro reti

Answer: D
Section: AUTOVALUTAZIONE

Q486. I principali protocolli del livello di trasferimento del Modello TCP/IP sono:

A. Il protocollo HTTP per il trasferimento di documenti Web, il protocollo SMTP per la posta elettronica, il protocollo FTP per il trasferimento di file tra sistemi remoti, il protocollo DNS per la conversione di indirizzi simbolici in indirizzi numerici IP

B. Il protocollo Ethernet che gestisce le trasmissioni nelle LAN

C. Il protocollo IP che gestisce l'instradamento dei pacchetti consentendo di interconnettere reti eterogenee per tecnologia, prestazioni e gestione

D. Il protocollo TCP che garantisce una trasmissione affidabile tra mittente e destinatario con ritrasmissione dei pacchetti persi, il protocollo UDP che fornisce una trasmissione con possibilità di perdita di pacchetti ma più veloce

Answer: D
Section: AUTOVALUTAZIONE

Q487. Il campo payload di un pacchetto gestito al livello di Collegamento è costituito da:
A. Un Segmento fornito dal livello di Trasporto
B. Un Frame fornito dal livello di Collegamento
C. Un Messaggio fornito dal livello di Applicazione
D. Un Datagramma fornito dal livello di Rete

Answer: D
Section: AUTOVALUTAZIONE

Q488. Quali di queste categorie non fa parte dei servizi di sicurezza:
A. Autenticazione
B. Privacy
C. Integrità dei dati
D. Segretezza dei dati

Answer: B
Section: AUTOVALUTAZIONE

Q489. Il servizio di autenticazione garantisce:
A. La riservatezza di una comunicazione
B. Lo scambio di chiavi
C. La segretezza dei dati
D. L'autenticità di una comunicazione

Answer: D
Section: AUTOVALUTAZIONE

Q490. Il seguente testo cifrato ASTENAIXTIUTTLAY secondo la tecnica di trasposizione a righe (4 righe e chiave K=3124) equivale al testo in chiaro:
A. Tanti saluti a x e y
B. Tanti saluti a te xy
C. Tanti saluti a tutti
D. Salutatemi tutti

Answer: B
Section: AUTOVALUTAZIONE

Q491. Quali di questi elementi non fa parte del modello di cifratura simmetrico:
A. Testo cifrato
B. Chiave segreta
C. Terza parte fidata
D. Algoritmo di decrittografia

Answer: C
Section: AUTOVALUTAZIONE

Q492. Nella cifratura di Giulio Cesare che cosa si può dire dell'attacco a forza bruta:
A. Non è efficace
B. La conoscenza della lingua del messaggio dà un vantaggio a questo tipo di attacco
C. Non serve conoscere l'algoritmo di cifratura
D. Funziona ma impiega molto tempo

Answer: B
Section: AUTOVALUTAZIONE

Q493. Nell'algoritmo DES i dati subiscono una permutazione iniziale:
A. Basata sulla chiave di 56 bit
B. Basata su una sottochiave
C. Basata su una tabella
D. Circolare a sinistra

Answer: C
Section: AUTOVALUTAZIONE

Q494. In cosa differiscono la crittografia di canale e quella end-to-end:
A. Sono la stessa cosa
B. Nell'uso della chiave segreta
C. Nella crittografia di canale la cifratura viene eseguita tra i terminali finali
D. Nella crittografia end-to-end la cifratura viene eseguita tra i terminali finali

Answer: D
Section: AUTOVALUTAZIONE

Q495. Nel protocollo di distribuzione delle chiavi, perché l'utente A invia un nonce:
A. Per identificare univocamente quella richiesta
B. Per identificarsi
C. Non invia un nonce
D. Per poi inviarlo all'utente B

Answer: A
Section: AUTOVALUTAZIONE

Q496. Uno dei principali usi della crittografia asimmetrica è:
A. La cifratura di messaggi
B. La distribuzione di certificati
C. La distribuzione delle chiavi pubbliche
D. La distribuzione delle chiavi segrete

Answer: D
Section: AUTOVALUTAZIONE

Q497. Qual è la differenza sostanziale fra un codice MAC e una funzione hash:
A. Non c'è differenza
B. La funzione hash non dipende da una chiave
C. Il codice MAC non dipende da una chiave
D. La funzione hash è invertibile

Answer: B
Section: AUTOVALUTAZIONE

Q498. Quale affermazione sulle funzioni di fase interne al modulo F è falsa:
A. Sono in numero di 80

B. Prendono in input il buffer dei registri
C. Producono in output il buffer dei registri
D. Prendono in input il buffer dei registri, la word di fase e la costante di fase

Answer: B
Section: AUTOVALUTAZIONE

Q499. Il file delle password generalmente contiene:
A. Le password cifrate
B. Nome utente cifrato e password in chiaro
C. Nome utente e password in chiaro
D. Nome utente e password cifrata

Answer: D
Section: AUTOVALUTAZIONE

Q501. Quali dei seguenti campi non fa parte del formato di un certificato X.509:
A. Numero seriale del certificato
B. Nome dell'emettitore
C. Chiave privata
D. Periodo di validità

Answer: C
Section: AUTOVALUTAZIONE

Q502. Una connessione SSL presenta le seguenti caratteristiche:
A. Può prevedere più servizi
B. Può essere stabilita all'interno di più sessioni
C. Viene stabilita all'interno di una singola sessione
D. Non condivide parametri di sicurezza con altre connessioni

Answer: C
Section: AUTOVALUTAZIONE

Q503. Le porte utilizzate da HTTP e HTTPS sono rispettivamente:
A. 25 e 443
B. 80 e 25
C. 80 e 443
D. 443 e 80

Answer: C
Section: AUTOVALUTAZIONE

Q504. Nella Purchase Response dello standard SET, il venditore invia:
A. Un blocco di conferma cifrato con la chiave pubblica del gateway di pagamento
B. Un blocco di conferma cifrato con la sua chiave pubblica
C. Un blocco di conferma cifrato con la sua chiave privata
D. Un blocco di conferma cifrato con la chiave monouso inviata dal cliente

Answer: C
Section: AUTOVALUTAZIONE

Q505. Il firewall non può effettuare filtraggio del traffico sulla base di:
A. Indirizzi IP
B. Tipologie di applicazioni
C. Tipologie di contenuti
D. Dati provenienti da reti wireless

Answer: D
Section: AUTOVALUTAZIONE

Q506. Il Digital Forensics è:
A. Una branca della scienza forense che estrae prove digitali dall'analisi del traffico di rete
B. Una branca della scienza forense che analizza immagini digitali
C. Una branca della scienza forense che analizza computer e dispositivi digitali
D. Una branca della scienza forense che analizza prove digitali recuperate da sorgenti digitali

Answer: D
Section: AUTOVALUTAZIONE

Q507. Quali delle seguenti affermazioni su Blockchain è errata:
A. Ogni blocco della catena dipende dal precedente
B. Ogni blocco della catena contiene informazioni su delle transazioni
C. Ogni blocco della catena contiene informazioni su delle transazioni ma non si vedono le cifre coinvolte
D. Le identità dei soggetti coinvolti nelle transazioni non sono in chiaro

Answer: C
Section: AUTOVALUTAZIONE

Q508. Un attaccante che modifica un blocco della Blockchain deve:
A. Un diverso nonce ma che cominci per 0
B. Usare lo stesso nonce ma un diverso hash valido
C. Ritrovare un nuovo nonce e conseguentemente un diverso hash valido
D. Ritrovare un nuovo nonce ma riprodurre lo stesso hash valido

Answer: C
Section: AUTOVALUTAZIONE

Q509. Nel protocollo Crowds, la richiesta del mittente:
A. Segue un percorso non casuale
B. Passa da un solo jondo del crowd
C. Attraversa tutti i proxy jondo del crowd
D. Attraversa alcuni proxy jondo del crowd

Answer: D
Section: AUTOVALUTAZIONE

Q510. Nel protocollo Crowds, un proxy jondo decide di inoltrare la richiesta ricevuta verso un altro jondo se:
A. La richiesta è già passata da un numero sufficiente di jondo
B. La richiesta contiene un'intestazione specifica
C. Il risultato del lancio di una moneta indica di inoltrare
D. Si è esaurito il numero di passaggi previsto

Answer: C
Section: AUTOVALUTAZIONE

Q510. La velocità di trasmissione di un collegamento in una rete di calcolatori è misurata in:
A. Numero totale di bit trasmessi
B. Tempo impiegato dall'invio alla ricezione del messaggio
C. Numero di bit al secondo
D. Numero totale di pacchetti trasmessi

Answer: C
Section: AUTOVALUTAZIONE

Q511. La denominazione ISP (Internet Service Provider) indica:
A. Un insieme di collegamenti e di commutatori di pacchetto gestito da una struttura commerciale o da un ente, che fornisce vari tipi di accesso a Internet tra cui quello residenziale a banda larga, senza fili (wireless) e in mobilità.
B. Il software che consente di pubblicare i siti Web in Internet.
C. Il modem che consente vari tipi di accesso a Internet tra cui quello senza fili (wireless)
D. L'insieme dei router in Internet che collegano le abitazioni degli utenti

Answer: A
Section: AUTOVALUTAZIONE

Q512. La denominazione Request For Comment indicata dalla sigla RFC è riferita a:
A. Il formato standard dei commenti inseriti nella progettazione delle pagine Web
B. Gli standard per Internet sviluppati dalla Internet Engineering Task Force (IETF)
C. Il formato standard dei commenti inseriti nel Software che gestisce la trasmissione a commutazione di pacchetto
D. Il formato standard dei commenti inseriti nel progetto Hardware di una rete di calcolatori

Answer: B
Section: AUTOVALUTAZIONE

Q513. Il buffer di output è:
A. Il dispositivo del router che contiene l'indirizzo della destinazione di un pacchetto che il router sta ricevendo fino a quando non si completa la ricezione
B. Un dispositivo di memoria della sorgente in cui sono memorizzati i bit di un pacchetto che la sorgente sta inviando fino a quando non si completa la ricezione.
C. Un dispositivo di memoria del router in cui memorizza i bit di un pacchetto che sta ricevendo fino a quando non si completa la ricezione, ed in cui i pacchetti già ricevuti sono messi in coda in attesa che il collegamento in uscita del router sia disponibile per la trasmissione
D. Un dispositivo di memoria della destinazione in cui il router memorizza i bit di un pacchetto che sta inviando fino a quando non si completa la ricezione.

Answer: C
Section: AUTOVALUTAZIONE

Q515. Se i pacchetti in arrivo ad un router per mancanza di spazio non possono essere memorizzati nel buffer di output in attesa di essere trasmessi sul collegamento di uscita occupato in una trasmissione, si ha che:
A. I pacchetti vengono memorizzati su un server messo a disposizione dal provider
B. Il router invia al provider una richiesta di spazio aggiuntivo di memorizzazione
C. Il router indirizza i pacchetti su un diverso collegamento di uscita libero

D. I pacchetti vengono eliminati e si ha una perdita di pacchetti per overflow del buffer di output

Answer: D
Section: AUTOVALUTAZIONE

Q516. Considerando solo il ritardo di trasmissione nella rete in figura, quando attraverso il collegamento comune di velocità R nel nucleo della rete, condiviso ad intervalli di tempo uguali, avvengono 10 trasmissioni di dati contemporane tra 10 coppie client-server , la velocità del collegamento comune disponibile per ogni trasferimento dati tra una coppia client-server è:
A. Il valore R/10 bps
B. Il valore R bps
C. Il valore 10R bps
D. Il valore 10/R bps

Answer: A
Section: AUTOVALUTAZIONE

Q517. I modelli di protocolli ISO/OSI e TCP/IP sono:
A. Diversi perché i livelli di Presentazione e di Sessione non sono presenti nello standard ISO/OSI
B. Diversi perché i livelli di Presentazione e di Sessione non sono presenti nello standard TCP/IP
C. Diversi per l'ordine gerarchico dei livelli dei protocoli
D. Denominazioni differenti di una stessa suite di protocolli di Internet

Answer: B
Section: AUTOVALUTAZIONE

Q518. Il campo payload di un pacchetto gestito al livello di Trasporto è costituito da:
A. Un Datagramma fornito dal livello di Rete
B. Un Segmento fornito dal livello di Trasporto
C. Un Messaggio fornito dal livello di Applicazione
D. Un Frame fornito dal livello di Collegamento

Answer: C
Section: AUTOVALUTAZIONE

Q519. Il campo payload di un pacchetto gestito al livello Fisico è costituito da:
A. Un Segmento fornito dal livello di Trasporto
B. Un Datagramma fornito dal livello di Rete
C. Un Messaggio fornito dal livello di Applicazione
D. Un Frame fornito dal livello di Collegamento

Answer: D
Section: AUTOVALUTAZIONE

Q520. Un attacco passivo tenta di:
A. Modificare le informazioni
B. Rilevare o utilizzare le informazioni del sistema ma non agisce sulle sue risorse
C. Alterare il funzionamento di un sistema
D. Inibire il funzionamento di un sistema

Answer: B

Section: AUTOVALUTAZIONE

Q521. In un attacco passivo di analisi del traffico:
A. Se il traffico è cifrato non ci sono problemi
B. Anche se il traffico è cifrato, l'attaccante riesce lo stesso a leggere il messaggio
C. Il destinatario si accorge dell'attacco
D. L'attaccante riesce ad estrarre informazioni sul tipo di trasmissione

Answer: D
Section: AUTOVALUTAZIONE

Q522. L'attacco "Testo in chiaro scelto" prevede:
A. La possibilità per il criptanalista di scegliere il testo in chiaro da cifrare
B. La conoscenza della lunghezza della chiave segreta
C. La possibilità per il criptanalista di scegliere il testo cifrato
D. La possibilità per il criptanalista di scegliere indistintamente il testo cifrato o quello in chiaro

Answer: A
Section: AUTOVALUTAZIONE

Q523. L'algoritmo DES:
A. Si basa sulla cifratura di Feistel
B. Esegue una cifratura a flusso
C. Non esegue permutazioni
D. Usa 56 sottochiavi

Answer: A
Section: AUTOVALUTAZIONE

Q525. Nella funzione S-box i 6 bit di input sono così usati nella tabella di permutazione:
A. Il 1° e il 6° indicano la colonna, mentre quelli dal 2° al 5° individuano la riga
B. Il 1° e il 2° indicano la riga, mentre quelli dal 3° al 6° individuano la colonna
C. Il 5° e il 6° indicano la riga, mentre quelli dal 1° al 4° individuano la colonna
D. Il 1° e il 6° indicano la riga, mentre quelli dal 2° al 5° individuano la colonna

Answer: D
Section: AUTOVALUTAZIONE

Q526. Quale delle seguenti affermazioni non è vera:
A. Il 3DES usa un'operazione di decifratura durante la cifratura
B. Il 3DES può usare anche due sole chiavi
C. Il 3DES applica tre volte il DES
D. Il 3DES è vulnerabile all'Attacco MitM

Answer: D
Section: AUTOVALUTAZIONE

Q527. Nella distribuzione semplice della chiave segreta fra due utenti A e B, cosa invia l'utente A all'utente B per iniziare il dialogo:
A. La sua chiave privata e il suo identificativo
B. La sua chiave pubblica

C. La sua chiave pubblica e il suo identificativo
D. La sua chiave pubblica e la chiave segreta di sessione da lui generata

Answer: C
Section: AUTOVALUTAZIONE

Q528. Un virus è un programma che:
A. Non è un programma
B. Modifica altri programmi e contenuti eseguibili alterandoli; effettua copie di se stesso
C. Non effettua copie di se stesso
D. Si propaga tramite la posta elettronica

Answer: B
Section: AUTOVALUTAZIONE

Q529. In Kerberos V4, il server TGS invia al client:
A. La chiave per dialogare con il server
B. Il Ticket per il server
C. La chiave per dialogare con il server e il Ticket per il server
D. L'ID del server

Answer: C
Section: AUTOVALUTAZIONE

Q530. Nel formato del certificato X.509, il campo "periodo di validità" contiene:
A. Non esiste tale campo
B. La data di inizio della validità
C. La data di fine della validità
D. La data di inizio e fine della validità

Answer: D
Section: AUTOVALUTAZIONE

Q531. In IPSec, nel protocollo ESP, il campo Padding serve fondamentalmente a:
A. Allineare le word dei campi nel pacchetto ESP
B. Si tratta di un campo opzionale
C. Adattare il campo Payload Data alle esigenze di lunghezza per la cifratura
D. Adattare il campo Payload Data alle esigenze di lunghezza per il calcolo del codice MAC

Answer: C
Section: AUTOVALUTAZIONE

Q532. In PGP, l'autenticazione non garantisce:
A. La compressione
B. La segretezza
C. La firma digitale
D. La provenienza del messaggio

Answer: B
Section: AUTOVALUTAZIONE

Q533. Il protocollo IPSec si basa sull'uso di extension header che:
A. Modificano l'intestazione IP
B. Precedono l'intestazione IP
C. Seguono l'intestazione IP
D. Cancellano l'intestazione IP

Answer: C
Section: AUTOVALUTAZIONE

Q534. In IPSec, quale dei seguenti protocolli fornisce crittografia e autenticazione combinata:
A. Authentication Header
B. Encapsulated Security Payload
C. Encapsulated Security Payload e Authentication Header
D. Nessun protocollo

Answer: B
Section: AUTOVALUTAZIONE

Q535. Nel protocollo SSL Record, la cifratura si applica a:
A. Al testo in chiaro/compresso, al codice MAC e all'intestazione
B. Al testo compresso
C. Al testo in chiaro
D. Al testo in chiaro/compresso e al codice MAC

Answer: D
Section: AUTOVALUTAZIONE

Q536. In Blockchain, la sicurezza è data da:
A. La rete P2P e il Ledger distribuito
B. La rete P2P
C. IL Ledger distribuito
D. Il grande numero di nodi presenti nella rete P2P

Answer: A
Section: AUTOVALUTAZIONE

Q537. Il processo di "mining" consiste in:
A. Recuperare Bitcoin distribuiti nella rete P2P
B. Risolvere la PoW e ottenere Bitcoin
C. Aggiornare la blockchain
D. Aggiornare il Ledger distribuito

Answer: B
Section: AUTOVALUTAZIONE

Q538. Stando ai dati di Giugno 2019, la dimensione della blockchain di Bitcoin era dell'ordine di:
A. 100 MB
B. 1 GB
C. 100 GB
D. 1 TB

Answer: C
Section: AUTOVALUTAZIONE

Q538. Una Rete di calcolatori è:
A. L'insieme di servizi quali navigazione nel Word Wide Web, posta elettronica, videoconferenze, ecc., disponibili per tutti o per una parte selezionata di utenti
B. Un insieme di dispositivi Hardware collegati l'uno con l'altro da appositi canali di comunicazione, che mediante opportuni Software permettono agli utenti lo scambio di informazioni e la condivisione di risorse e di servizi
C. Un sistema Software complesso che permette agli utenti lo scambio di informazioni e la condivisione di risorse e servizi
D. Il WWW (Word Wide Web)

Answer: B
Section: AUTOVALUTAZIONE

Q539. L'idea base del protocollo Crowds è quella di:
A. Nascondere le comunicazioni di un utente facendole passare casualmente in un gruppo di utenti simili
B. Nascondere le comunicazioni di un utente facendole passare da un proxy
C. Nascondere le comunicazioni di un utente facendole passare sempre dagli stessi utenti del crowd
D. Annidare le comunicazioni secondo la tecnica di onion routing

Answer: A
Section: AUTOVALUTAZIONE

Q539. Una rete di accesso:
A. Connette fisicamente un sistema periferico al suo edge router (router di bordo) che è il primo router sul percorso che parte dal sistema di origine verso un qualsiasi altro sistema di destinazione collocato al di fuori della stessa rete di accesso
B. Connette fisicamente il nucleo della rete all'edge router (router di bordo) che è il primo router sul percorso che parte dal sistema di origine verso un qualsiasi altro sistema di destinazione
C. Connette un sistema periferico ad un server mediante una password di autenticazione
D. Connette un sistema periferico al servizio di posta elettronica

Answer: A
Section: AUTOVALUTAZIONE

Q540. In una trasmissione store and forward il tempo di trasmissione di un pacchetto di L bit dalla sorgente al router su un collegamento con velocità di trasmissione R bps è:
A. L-R secondi
B. 2L/R secondi
C. L/R secondi
D. L-2R secondi

Answer: C
Section: AUTOVALUTAZIONE

Q541. Quando il traffico relativo ad un collegamento di uscita da un router, misurato come rapporto tra il numero medio di bit ricevuti e il numero di bit inviati nell'unità di tempo, risulta minore o uguale a 1 si ha che:
A. Il ritardo medio di accodamento è limitato superiormente da un valore finito
B. Il ritardo medio di accodamento cresce linearmente al tendere a 1 del valore del rapporto che misura il traffico
C. Il ritardo medio di accodamento cresce esponenzialmente al tendere a 1 del valore del rapporto che misura il

traffico
D. Il ritardo medio di accodamento è costante

Answer: C
Section: AUTOVALUTAZIONE

Q542. Considerando solo il ritardo di trasmissione nella rete in figura dove R1 bps,& , RN bps sono le velocità dei collegamenti attraversati nella trasmissione dei dati , il throughput medio end-to-end di una trasmissione di dati tra client e server è approssimato da:
A. Throughput medio end-to-end = massimo(R1,& ,RN) bps
B. Throughput medio end-to-end = (R1+& +RN)/N bps
C. Throughput medio end-to-end = minimo(R1, ..., RN) bps
D. Throughput medio end-to-end = R1+& +RN bps

Answer: C
Section: AUTOVALUTAZIONE

Q543. In una rete di calcolatori, la misura del throughput medio end-to-end di una trasmissione di dati tra due sistemi periferici è espressa in:
A. Bit
B. Bit al secondo
C. Metri al secondo
D. Secondi

Answer: B
Section: AUTOVALUTAZIONE

Q545. Un malware è:
A. Un Software per impedire un attacco sul computer di un utente attraverso una attività svolta in rete
B. Un Software dannoso che l'autore di un attacco può installare sul computer di un utente attraverso una attività svolta in rete
C. Un dispositivo Harware per impedire un attacco sul computer di un utente attraverso una attività svolta in rete
D. Gli strumenti Hardware e Software utilizzati per impedire gli attacchi mediante attività svolte in rete

Answer: B
Section: AUTOVALUTAZIONE

Q547. Nel caso di chiave a 56 bit, l'attacco a forza bruta (106 crittografie/µs), per avere successo, impiega:
A. circa 10 minuti
B. circa 10 ore
C. circa 10 giorni
D. circa 10 anni

Answer: B
Section: AUTOVALUTAZIONE

Q549. La crittografia multipla consiste in:
A. Applicare più volte la stessa chiave
B. Applicare più volte l'algoritmo di cifratura ma non di decifratura
C. Applicare più volte uno stesso algoritmo
D. Applicare in sequenza algoritmi di cifratura diversi

Answer: C
Section: AUTOVALUTAZIONE

Q551. Le modalità di funzionamento della cifratura definiscono:
A. La tipologia di algoritmo da usare
B. Come vengono eseguite in sequenza le operazioni di cifratura
C. Il numero e la dimensione dei blocchi
D. La generazione delle chiavi di cifratura

Answer: B
Section: AUTOVALUTAZIONE

Q552. Nella modalità Electronic Codebook non si usa:
A. Sempre la stessa chiave
B. Cifratura e decifratura diverse
C. Bit di riempimento
D. Blocchi di dimensione diversa

Answer: D
Section: AUTOVALUTAZIONE

Q553. Nella modalità Cipher Feedback cosa viene messo in input alla funzione di crittografia:
A. Un registro a scorrimento di s bit (dimensione segmento) e la chiave K
B. Un registro a scorrimento di b bit (dimensione blocco)e la chiave K
C. Il testo in chiaro e la chiave K
D. Il testo cifrato al passo precedente e la chiave K

Answer: B
Section: AUTOVALUTAZIONE

Q554. La principale complessità della crittografia di canale riguarda:
A. Non ci sono complessità
B. La necessità di un grande numero di dispositivi di crittografia e di chiavi
C. La vulnerabilità agli attacchi
D. La dimensione del blocco dati

Answer: B
Section: AUTOVALUTAZIONE

Q555. Nella distribuzione delle chiavi segrete, si usa la crittografia asimmetrica perché:
A. Poi si può usare la crittografia simmetrica che è più veloce
B. Non è vero, si fa l'opposto
C. Poi si può usare la crittografia simmetrica che è più sicura
D. Non ci sono altri modi per scambiarsi le chiavi segrete

Answer: A
Section: AUTOVALUTAZIONE

Q556. Nello scambio di chiavi Diffie-Hellman, i valori q e a sono:
A. Primi fra loro

B. Il valore q è un numero primo e a è un valore intero
C. Due valori primi
D. Il valore q è un numero primo e a è un valore casuale

Answer: B
Section: AUTOVALUTAZIONE

Q557. Nell'algoritmo HMAC, l'input del primo hash è costituto da:
A. L blocchi
B. (L-1) blocchi
C. (L+1) blocchi
D. (L+b) blocchi

Answer: C
Section: AUTOVALUTAZIONE

Q559. In Kerberos V4 il TGS ha la funzione di:
A. Autenticare l'utente in una sessione
B. Consentire all'utente di accedere ad un altro servizio all'interno della stessa sessione
C. Consentire all'utente di accedere ad un'altra sessione senza reimmettere la password
D. Custodire le password degli utenti

Answer: B
Section: AUTOVALUTAZIONE

Q560. In Kerberos V4, il server, per garantire reciproca autenticazione, può inviare al client:
A. Un timestamp cifrato con la sua chiave privata
B. Il timestamp inviato dal client, incrementato di 1 e cifrato con la chiave tra loro condivisa
C. Il timestamp inviato dal client incrementato di 1 non cifrato
D. Un timestamp cifrato con la chiave tra loro condivisa

Answer: B
Section: AUTOVALUTAZIONE

Q561. In una rete di calcolatori, il tempo di una trasmissione di dati tra due sistemi periferici che si ricava dall'espressione del throughput medio end-to-end è dato da:
A. Tempo = throughput/F secondi, dove F è il numero di bit trasmessi tra i due sistemi periferici
B. Tempo = F/throughput secondi, dove F è il numero di bit trasmessi tra i due sistemi periferici
C. Tempo = 2F/throughput secondi, dove F è il numero di bit trasmessi tra i due sistemi periferici
D. Tempo = F+throughput secondi, dove F è il numero di bit trasmessi tra i due sistemi periferici

Answer: B
Section: AUTOVALUTAZIONE

Q562. In SSL, il protocollo Change Cipher Spec specifica:
A. Di effettuare la decifratura
B. Di non effettuare la cifratura
C. Di cambiare la tipologia di cifratura
D. Di mantenere la tipologia di cifratura in uso

Answer: C

Section: AUTOVALUTAZIONE

Q562. La gestione di un IXP (Internet exchange Point) è:
A. Affidata agli ISP che gestiscono l'accesso degli utenti finali
B. Affidata agli ISP di livello 1
C. Di tipo commerciale, in cui l azienda che ha creato e che gestisce l IXP offre a pagamento i servizi agli ISP che ne diventano clienti, oppure di tipo consortile, in cui gli ISP che intendono stabilire un collegamento di tipo peering si riuniscono in associazioni e partecipano alla gestione dell IXP
D. Affidata all'ISP a cui appartiene il router che effettua lo smistamento del traffico dati

Answer: C
Section: AUTOVALUTAZIONE

Q563. Il protocollo TLS si presenta rispetto a SSL:
A. Identico
B. TLS è un'evoluzione di SSL
C. SSL è un'evoluzione di TLS
D. SSL è un sottoprotocollo di TLS

Answer: B
Section: AUTOVALUTAZIONE

Q563. In una rete a commutazione di pacchetto basata sull'Architettura a livelli l'incapsulamento è:
A. L'operazione che inserisce, nel campo payload di un pacchetto relativo ad un livello, il pacchetto gestito dal livello superiore
B. L'operazione che inserisce, nel campo payload del pacchetto relativo ad un livello, le informazioni aggiuntive gestite dai protocolli di tale livello
C. L'ordinamento nella pila (stack) dei livelli che costituiscono la suite di protocolli dell'Architettura
D. La memorizzazione dei pacchetti nel buffer di output di un router

Answer: A
Section: AUTOVALUTAZIONE

Q564. La caratteristica principale dei worm è:
A. Usare la posta elettronica per diffondersi
B. Non utilizzare le connessioni di rete
C. Propagarsi in maniera attiva
D. Usare i media digitali per diffondersi

Answer: C
Section: AUTOVALUTAZIONE

Q564. Una DoS provocata da una inondazione di connessione è:
A. Una interruzione del servizio causata da una gran numero di connessioni TCP generate dall'attaccante e mantenute tutte aperte per ingorgare la capacità ricettiva del server
B. Una interruzione del servizio causata dall'invio di una sequenza di pacchetti opportunamente costruiti ad una applicazione vulnerabile o al Sistema Operativo in esecuzione sul server sotto attacco, in grado di determinare il blocco del servizio o anche lo spegnimento del server
C. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server
D. La diffusione in rete di copie dei file memorizzati su un computer

Answer: A
Section: AUTOVALUTAZIONE

Q565. Quale delle seguenti definizioni descrive meglio il Backdoor:
A. Servizio di rete
B. Punto di accesso segreto di un programma che viene individuato da un hacker
C. Punto di accesso con livello più basso di segretezza verso un sistema
D. Punto di accesso verso un programma conosciuto da pochi

Answer: B
Section: AUTOVALUTAZIONE

Q565. La difesa da una attività di packet sniffing è costituita:
A. Dalla installazione di opportuni dispositivi Hardware
B. Dall'uso di tecniche di crittografia per codificare i messaggi trasmessi
C. Dal controlo del numero di accessi alla rete effettuati dal computer
D. Dal settaggio di opportuni paramentri di trasmissione dei messaggi nel sistema periferico sorgente

Answer: B
Section: AUTOVALUTAZIONE

Q567. Il servizio di Non Ripudiabilità impedisce che:
A. Il messaggio sia modificato
B. Il destinatario conosca il mittente
C. Il mittente possa inviare più messaggi
D. Il mittente neghi di aver inviato il messaggio

Answer: D
Section: AUTOVALUTAZIONE

Q568. Il seguente testo cifrato BOAOTNUNFRUA secondo la tecnica Rail Fence equivale al testo in chiaro:
A. Tanti auguri
B. Buonanotte
C. Buona fortuna
D. Buona serata

Answer: C
Section: AUTOVALUTAZIONE

Q571. Quale delle seguenti espressioni identifica la compatibilità tra 3DEs e DES:
A. C=E(K1,D(K1,E(K1,P)))
B. C=E(K1,E(K1,E(K1,P)))
C. C=E(K1,D(K1,E(K1,C)))
D. C=E(K1,E(K1,P))

Answer: A
Section: AUTOVALUTAZIONE

Q572. Nel caso di utilizzo della crittografia asimmetrica per la funzione di segretezza:
A. Il mittente usa in cifratura la chiave privata del destinatario

B. Il mittente usa in cifratura la sua chiave pubblica
C. Il mittente usa in cifratura la chiave pubblica del destinatario
D. Il mittente usa in cifratura la sua chiave privata

Answer: C
Section: AUTOVALUTAZIONE

Q573. Nel caso di utilizzo della crittografia asimmetrica per la funzione di autenticazione, un eventuale attaccante può riuscire a stimare:
A. La chiave privata del destinatario
B. Il testo in chiaro
C. La chiave pubblica del mittente
D. La chiave privata del mittente

Answer: D
Section: AUTOVALUTAZIONE

Q574. In RSA, cosa permette di fare l'algoritmo di Miller-Rabin:
A. Non serve
B. Determinare Õ(n)
C. Determinare n
D. Determinare i numeri primi p e q

Answer: D
Section: AUTOVALUTAZIONE

Q575. La firma digitale per l'autenticazione soddisfa il requisito:
A. Ripudio del destinatario
B. Ripudio del mittente
C. Segretezza
D. Ripudio mittente e destinatario

Answer: B
Section: AUTOVALUTAZIONE

Q576. Supponiamo di avere un codice MAC con una chiave lunga k=64 bit e un checksum lungo n=16 bit, quante coppie messaggio-checksum dovrebbe conoscere in media un attaccante per riuscire a individuare la chiave con un attacco a forza bruta:
A. 64
B. 4
C. 16
D. 256

Answer: B
Section: AUTOVALUTAZIONE

Q577. Quale dei seguenti non è un requisito dei codici MAC:
A. Deve essere computazionalmente impossibile che, dato il messaggio M e C(K,M), trovare un messaggio M' con C(K,M') = C(K,M)
B. Indicato con n il numero di bit di un codice MAC, la probabilità di collisione deve essere 1/2n
C. Indicato con n il numero di bit di un codice MAC, la probabilità di collisione deve essere 1/n

D. Dati due messaggi M e M' deve essere improbabile che C(k,M)= C(k,M')

Answer: C
Section: AUTOVALUTAZIONE

Q578. Le funzioni di fase interne al modulo F eseguono sostanzialmente:
A. Operazioni logiche
B. Operazioni AND e XOR
C. Permutazioni
D. Operazioni logiche, shift e somme modulari

Answer: D
Section: AUTOVALUTAZIONE

Q579. I codici MAC basati su algoritmi di crittografia e cifratura a blocchi possono superare le loro debolezze in termini di sicurezza tramite:
A. Aumentando il numero di crittografie effettuate
B. L'introduzione di una doppia chiave generata a partire da una singola
C. L'introduzione di due chiavi diverse
D. Cambiando algoritmo crittografico

Answer: B
Section: AUTOVALUTAZIONE

Q580. Con il termine "malware" si intende:
A. Un virus informatico
B. un programma nascosto all interno di un altro o indipendente, creato per compiere azioni illegittime e dannose
C. Un attacco informatico
D. Un programma infettato

Answer: B
Section: AUTOVALUTAZIONE

Q582. In PGP, la segretezza è fornita attraverso:
A. La cifratura simmetrica
B. La cifratura asimmetrica
C. Hash SHA-1
D. La compressione ZIP

Answer: A
Section: AUTOVALUTAZIONE

Q583. Il simbolo della tecnologia Wi-Fi utilizzata nelle reti WLAN:
A. Indica che il dispositivo è di tipo wireless
B. Indica che il dispositivo consente un collegamento satellitare
C. Rappresenta la certificazione rilasciata dal provider che garantisce la possibilità di connettere il dispositivo wireless ad una rete in fibra ottica basata sullo standard IEEE 802.11
D. Rappresenta la certificazione rilasciata dalla Wi-Fi Alliance che garantisce la interoperabilità dei dispositivi wireless basati sullo standard IEEE 802.11 prodotti da costruttori di Hardware diversi

Answer: D

Section: AUTOVALUTAZIONE

Q585. Quale tipo di firewall esercita il filtraggio sulla base delle applicazioni consentite:
A. A pacchetti
B. Proxy a livello di applicazione
C. A ispezione di stati
D. Controllo indirizzi IP

Answer: B
Section: AUTOVALUTAZIONE

Q585. In una rete a commutazione di pacchetto il ritardo di trasmissione relativo ad un collegamento in uscita di un router è il tempo:
A. Che il segnale impiega per percorrere il collegamento dato dal valore del rapporto d/v, dove d è la lunghezza in metri del collegamento che il pacchetto in uscita dal router deve percorrere per giungere al nodo successivo della rete, e v è la velocità in metri al secondo con cui viaggia il segnale caratteristica del materiale di cui è fatto il collegamento
B. Impiegato dal router per instradare il pacchetto verso il collegamento, dato dal valore del rapporto L/R, dove L è la lunghezza in bit del pacchetto ed R è la velocità di trasmissione in bit per secondi del collegamento in uscita dal router
C. Impiegato dal router per esaminare l intestazione del pacchetto e determinare su quale collegamento di uscita dirigerlo, più altro tempo eventuale per il controllo degli errori avvenuti nella trasmissione dei bit
D. Che un pacchetto impiega per raggiungere il sistema periferico di destinazione

Answer: B
Section: AUTOVALUTAZIONE

Q586. Cosa permette la proprietà "no write down":
A. Un soggetto di livello 3 non può leggere in un documento di livello 2
B. Un soggetto di livello 2 non può leggere in un documento di livello 3
C. Un soggetto di livello 2 non può scrivere in un documento di livello 3
D. Un soggetto di livello 3 non può scrivere in un documento di livello 2

Answer: C
Section: AUTOVALUTAZIONE

Q587. Esistono tecniche di MM Forensics che permettono di stabilire se:
A. Un'immagine proviene da una fotocamera o da uno scanner
B. Un'immagine proviene da una fotocamera o da una chiave USB
C. Un'immagine proviene da una fotocamera ma non è vero per i video
D. Un video proviene da una fotocamera ma non è vero per le immagini statiche

Answer: A
Section: AUTOVALUTAZIONE

Q588. Nel MM Forensics, quali sono generalmente le fasi operative per la localizzazione in un'immagine di un attacco copy-move:
A. Calcolo dei descrittori, matching, clustering e localizzazione
B. Calcolo dei descrittori e localizzazione
C. Calcolo dei descrittori, clustering e localizzazione
D. Calcolo dei descrittori, filtraggio, clustering e localizzazione

Answer: A

Section: AUTOVALUTAZIONE

Q588. Il livello di Applicazione dello standard ISO/OSI offre servizi:
A. Di crittografia e di compressione del testo
B. Per consentire alle applicazioni di interpretare il significato semantico dei dati
C. Per i processi relativi all esecuzione delle applicazioni sui sistemi periferici sorgente e destinazione
D. Che consentono la sincronizzazione dello scambio dei dati

Answer: C
Section: AUTOVALUTAZIONE

Q589. Il livello di Rete dello standard ISO/OSI offre servizi:
A. Per il trasferimento di dati tra nodi adiacenti attraverso il tipo di collegamento che sussiste tra di loro
B. Che permettono un trasferimento di dati affidabile, effettuando anche un controllo degli errori e delle perdite di pacchetti tra due sistemi periferici
C. Che consentono la comunicazione tra i nodi della rete che vengono attraversati nel percorso che va dal sistema periferico sorgente al sistema periferico destinazione
D. Necessari a livello Hardware per controllare il flusso di dati attraverso i collegamenti e le connessioni ai dispositivi che permettono il passaggio dei segnali che rappresentano le informazioni

Answer: C
Section: AUTOVALUTAZIONE

Q591. La cifratura di Vernam prevede:
A. Una decifratura con un'operazione diversa da quella in cifratura
B. Una chiave lunga quanto il testo in chiaro e un'operazione di OR
C. Una cifratura a blocchi
D. Una chiave lunga quanto il testo in chiaro e un'operazione di XOR

Answer: D
Section: AUTOVALUTAZIONE

Q594. Nella parametrizzazione di AES, una word corrisponde a:
A. 32 bit
B. 64 bit
C. 128 bit
D. 16 bit

Answer: A
Section: AUTOVALUTAZIONE

Q596. Quale fra le seguenti non è una modalità di cifratura:
A. Cipher Block Chaining
B. Electronic Codebook
C. Output chaining
D. Counter

Answer: C
Section: AUTOVALUTAZIONE

Q598. Quale proprietà dell'aritmetica modulare si usa in RSA nella cifratura/decifratura

A. [(a mod n)*(b mod n)] mod n =1 mod n
B. [(a mod n)*(b mod n)] mod n =(a*b) mod n
C. [(a mod n)*(b mod n)] mod n =n mod n
D. [(a mod n)*(b mod n)] mod n =ab

Answer: B
Section: AUTOVALUTAZIONE

Q599. Nel caso di "attacco a compleanno" nei confronti di un codice hash a 48 bit, l'attaccante deve generare un numero di messaggi fraudolenti F pari a:
A. F=296
B. F=216
C. F=224
D. F=248

Answer: C
Section: AUTOVALUTAZIONE

Q600. Il "paradosso del compleanno" stabilisce che:
A. Esiste una probabilità del 50% che in un gruppo di circa 23 persone ve ne siano due coetanee
B. Esiste una probabilità del 50% che in un gruppo di circa 23 persone ve ne siano due nate lo stesso giorno
C. Esiste una probabilità del 50% che in un gruppo di circa 50 persone ve ne siano due nate lo stesso giorno
D. Esiste una probabilità del 23% che in un gruppo di circa 50 persone ve ne siano due nate lo stesso giorno

Answer: B
Section: AUTOVALUTAZIONE

Q601. Nell'algoritmo HMAC, la funzione di hash viene utilizzata:
A. 1 volta
B. 2 volte con vettore di inizializzazione uguale
C. 2 volte con vettore di inizializzazione diverso
D. 3 volte

Answer: B
Section: AUTOVALUTAZIONE

Q602. Nell'algoritmo HMAC, la chiave K+ viene usata:
A. Direttamente come input per la funzione di hash
B. Non viene usata
C. Come input per lo XOR con il messaggio
D. Integrata nel messaggo come input per la funzione di hash

Answer: D
Section: AUTOVALUTAZIONE

Q602. Un worm informatico è:
A. Un malware autoreplicante che richiede una qualche forma di interazione con l utente per poter infettare il dispositivo
B. Un malware autoreplicante che può infettare un dispositivo senza alcuna interazione esplicita con l utente
C. La rete di computer infettati che l autore di un attacco controlla
D. Un Software che copia sul computer dell'attaccante i file memorizzati sul computer di un utente inconsapevole

Answer: B
Section: AUTOVALUTAZIONE

Q603. Nella funzione di Shift rows:
A. Si eseguono degli spostamenti circolari a destra
B. Si eseguono degli spostamenti circolari a destra e a sinistra
C. Si eseguono degli spostamenti circolari a destra di un byte
D. Si eseguono degli spostamenti circolari a sinistra ma la prima riga non cambia

Answer: D
Section: AUTOVALUTAZIONE

Q604. Indicare quale relazione descrive l'Attacco MitM:
A. E(K1,P)=D(K2,C)
B. E(K1,P)=D(K1,C)
C. E(K2,P)=D(K2,C)
D. E(K1,P)=E(K2,C)

Answer: A
Section: AUTOVALUTAZIONE

Q605. Indicare l'espressione corretta per la cifratura 3DES:
A. C=E(K1,D(K2,E(K1,P)))
B. C=E(K1,E(K2,E(K1,P)))
C. C=E(K1,D(K2,E(K2,P)))
D. C=E(K1,D(K1,E(K1,P)))

Answer: A
Section: AUTOVALUTAZIONE

Q606. Il protocollo IPSec consente di:
A. Bloccare tutti gli attacchi
B. Impedire il monitoraggio non autorizzato del traffico
C. Impedire l'accesso da remoto su una rete aziendale
D. Impedire il trasferimento di file da remoto su una rete aziendale

Answer: B
Section: AUTOVALUTAZIONE

Q606. Nella modalità Counter, quale di queste affermazioni è sbagliata:
A. Cifratura e decifratura sono la stessa funzione
B. Il valore di ciascun contatore non cambia da blocco a blocco
C. Il valore del contatore viene cifrato e messo in XOR con il testo in chiaro
D. Non esiste alcuna concatenazione tra i vari passi

Answer: B
Section: AUTOVALUTAZIONE

Q607. Nel protocollo SSL Record, il servizio di integrità del messaggio è realizzato mediante:
A. Hash

B. Codice MAC
C. RSA
D. Cifratura simmetrica

Answer: B
Section: AUTOVALUTAZIONE

Q608. La sicurezza multilivello indica:
A. Una politica di sicurezza a strati
B. Una politica di sicurezza in cui le informazioni sono accessibili sulla base di diversi livelli gerarchici
C. Una politica di sicurezza con controlli gerarchici
D. Una politica di sicurezza che implica più livelli di controllo

Answer: B
Section: AUTOVALUTAZIONE

Q608. Quali operazioni complesse deve effettuare un utente in RSA:
A. La scelta dei numeri primi p e q
B. La scelta dei numeri primi n e q
C. La scelta dei numeri primi n e p
D. Nessuna operazione complessa

Answer: A
Section: AUTOVALUTAZIONE

Q609. Il rumore PRNU presenta le seguenti caratteristiche:
A. Moltiplicativo e sistematico
B. Moltiplicativo e dipendente dalla temperatura
C. Moltiplicativo e dipendente dal tempo
D. Sistematico e additivo

Answer: A
Section: AUTOVALUTAZIONE

Q610. Nel caso di uso di tecniche di MM Forensics in applicazioni per il cyberbullismo,si può riuscire a:
A. Rintracciare in rete la foto/video di un atto di bullismo
B. Determinare un collegamento tra il dispositivo di acquisizione di una foto/video di un atto di bullismo e la foto/video stesso
C. Determinare un collegamento diretto tra l'autore di una foto/video di un atto di bullismo e la foto/video stesso
D. Eviatre la condivisione in rete di una foto/video di un atto di bullismo

Answer: B
Section: AUTOVALUTAZIONE

Q610. Nello scambio di chiavi Diffie-Hellman, i valori q e a sono:
A. Entrambi pubblici
B. Solo uno dei due è pubblico
C. Il valore q è pubblico ma a è privato
D. Entrambi privati

Answer: A

Section: AUTOVALUTAZIONE

Q611. Nell'accesso ai "servizi nascosti" della rete Tor, i punti di introduzione sono:
A. Punti di accesso alla rete Tor
B. Dei Tor relay su cui accedere ad un "servizio nascosto"
C. Dei Tor relay su cui il "servizio nascosto" espone il proprio servizio
D. Dei server di guardia

Answer: C
Section: AUTOVALUTAZIONE

Q611. Con la sola funzione hash si riesce a garantire:
A. La segretezza
B. La firma digitale
C. L'autenticazione ma le due parti devono condividere un valore segreto
D. La segretezza ma le due parti devono condividere un valore segreto

Answer: C
Section: AUTOVALUTAZIONE

Q612. Nel caso di funzione hash basata sullo XOR di 4 blocchi di messaggio, ciascuno da 3 bit, si ha che:
A. L'hash è costituto da 3 bit
B. L'hash è costituto da 4 bit
C. L'hash è costituto da 12 bit
D. L'hash è costituto da 7 bit

Answer: A
Section: AUTOVALUTAZIONE

Q615. Quale delle seguenti affermazioni è falsa:
A. Tutti i malware sono programmi software
B. Tutti i malware devono essere trasferiti in un sistema
C. Tutti i malware si replicano
D. Non sempre i malware compiono azioni dannose sui file

Answer: C
Section: AUTOVALUTAZIONE

Q617. In IPSec, nel protocollo ESP, il campo Authentication Data è generato:
A. Tramite un codice MAC
B. Tramite un hash
C. Tramite cifratura RSA
D. Tramite un'operazione di XOR sui campi precedenti

Answer: A
Section: AUTOVALUTAZIONE

Q618. In una rete di accesso a Internet DSL il DSLAM (Digital Subscriber Line Access Multiplexer) che si trova nella centrale locale della compagnia telefonica effettua:
A. Il multiplexing raccogliendo i dati provenienti dalle abitazioni e istadandoli su un unico collegamento verso l'ONT (Optical Network Terminator) che costituisce l'edge router del collegamento alla rete

B. Il multiplexing del segnale proveniente dalla linea telefonica esterna all'abitazione, separando il segnale analogico del traffico vocale dal segnale analogico del traffico dati, e invia questi segnali all apparecchio telefonico ed al modem mediante collegamenti separati
C. Il multiplexing del segnale proveniente dalla linea telefonica esterna all'abitazione, separando il segnale analogico del traffico vocale dal segnale analogico del traffico dati, e invia i dati all'ONT (Optical Network Terminator) che fornisce la conversione tra segnali ottici e segnali elettrici digitali
D. Il multiplexing raccogliendo i dati provenienti dalle abitazioni e istadandoli su un unico collegamento verso il router dell'operatore telefonico, la conversione dei dati da analogico a digitale e la divisioni dei segnali vocali e dei dati digitali istradandoli verso le rispettive reti.

Answer: D
Section: AUTOVALUTAZIONE

Q619. In IPSec per Associazione di Sicurezza si intende:
A. Una relazione bidirezionale fra un mittente e un destinatario riguardante i servizi di sicurezza
B. Una relazione monodirezionale fra un mittente e un destinatario riguardante i servizi di sicurezza
C. Un servizio di sicurezza
D. Una relazione monodirezionale fra un mittente e un destinatario per lo scambio delle chiavi di cifratura

Answer: B
Section: AUTOVALUTAZIONE

Q620. In IPSec, il campo Sequence Number nell'Authetication Header serve a:
A. Inserire un valore casuale
B. Soltanto a numerare i pacchetti IP
C. Impedire attacchi replay
D. A tenere conto dei pacchetti IP passati

Answer: C
Section: AUTOVALUTAZIONE

Q620. L'overflow del buffer di output di un router determina:
A. L'errore nella determinazione del collegamento di uscita su cui instradare un pacchetto in arrivo
B. L'invio di un messaggio al provider per segnalare la mancanza di memoria disponibile per l'esecuzione delle operazioni previste dai protocolli
C. La perdita dei pacchetti in arrivo al router che non possono essere memorizzati nella coda di attesa della trasmissione su un collegamento in uscita
D. L'errore nella determinazione dell'indirizzo IP del sistema periferico destinazione di un pacchetto in arrivo

Answer: C
Section: AUTOVALUTAZIONE

Q621. Nel protocollo TLS, la funzione pseudo-random può essere:
A. Iterata più volte per ottenere il numero di dati necessario
B. Iterata due volte
C. Iterata ma solo per un numero di volte definito dal protocollo stesso
D. Non può essere iterata

Answer: A
Section: AUTOVALUTAZIONE

Q622. Nello standard SET, la doppia firma serve a:
A. A collegare due messaggi per due diversi destinatari ma provenienti da stesso mittente
B. Ad inviare le informazioni dell'ordine
C. Ad inviare le informazioni del pagamento
D. A garantire il venditore

Answer: A
Section: AUTOVALUTAZIONE

Q622. Un attacco attivo prevede:
A. La modifica del flusso dei dati o la creazione di un flusso falsificato
B. Necessariamente l'interazione con il mittente del messaggio
C. La precedente realizzazione di un attacco passivo
D. Necessariamente l'accesso ai dati trasmessi

Answer: A
Section: AUTOVALUTAZIONE

Q623. Quale servizio si occupa di proteggere il flusso dei dati dall'analisi:
A. Crittografia
B. Segretezza del traffico
C. Autenticazione dell'entità peer
D. Integrità dei dati

Answer: B
Section: AUTOVALUTAZIONE

Q625. Il principale scopo del firewall è:
A. Proteggere la rete interna da eventuali attacchi esterni
B. Proteggere la rete interna da eventuali attacchi interni
C. Proteggere un singolo host della rete interna da eventuali attacchi
D. Proteggere due host reciprocamente

Answer: A
Section: AUTOVALUTAZIONE

Q626. I 64 bit in input a ciascuna fase:
A. Vengono divisi in due metà, di cui una non viene elaborata ma solo scambiata di posto
B. Vengono divisi in due metà che subiscono la stessa elaborazione
C. Vengono divisi in due metà, di cui una non cambia di posizione
D. Non vengono divisi in due metà

Answer: A
Section: AUTOVALUTAZIONE

Q627. Nell'analisi di un contenuto multimediale, le tecniche di MM Forensics di solito dispongono di:
A. Un contenuto di riferimento
B. Nessun contenuto di riferimento
C. Del contenuto originale
D. Della fotocamera

Answer: B
Section: AUTOVALUTAZIONE

Q627. L'algoritmo AES si basa su:
A. Fasi composte da blocchi di Feistel
B. Fasi composte da due funzioni
C. Fasi composte da quattro funzioni
D. Fasi composte da funzioni di permutazione

Answer: C
Section: AUTOVALUTAZIONE

Q628. Esistono tecniche di MM Forensics che consentono di determinare se un'immagine digitale è:
A. Contraffatta e di localizzare l'eventuale alterazione
B. Contraffatta ma solo in presenza dell'originale
C. Contraffatta ma solo se di alta qualità
D. Autentica ma solo tramite un'operazione di confronto

Answer: A
Section: AUTOVALUTAZIONE

Q629. Lo svantaggio principale della modalità Electronic Codebook è:
A. La necessità di usare bit di riempimento
B. L'uso della stessa chiave
C. La semplicità di cifratura
D. Lo stesso blocco di testo in chiaro produce lo stesso blocco di testo cifrato

Answer: D
Section: AUTOVALUTAZIONE

Q630. Nella modalità Cipher Block Chaining come si risolvono i problemi di sicurezza di ECB:
A. Utilizzando un vettore di inizializzazione
B. Mettendo in input il testo cifrato al passo precedente
C. Cambiando la chiave ad ogni passo
D. Rendendo cifratura e decifratura uguali

Answer: B
Section: AUTOVALUTAZIONE

Q631. Nella modalità Cipher Block Chaining quali requisiti ci sono sul vettore di inizializzazione:
A. Deve essere generato dalla chiave
B. Deve essere cambiato ad ogni passo
C. Deve essere noto al destinatario
D. Nessun requisito

Answer: C
Section: AUTOVALUTAZIONE

Q634. La crittografia asimmetrica prevede:
A. L'uso di due chiavi segrete
B. L'uso di una chiave segreta

C. L'uso di due chiavi di cui una privata
D. L'uso di due chiavi pubbliche

Answer: C
Section: AUTOVALUTAZIONE

Q635. Un router è:
A. Un commutatore di pacchetto usato nelle reti di accesso
B. Un host che scambia messaggi suddivisi in pacchetti con un dispositivo remoto connesso in rete
C. Un sistema periferico che scambia messaggi suddivisi in pacchetti con un dispositivo nel nucleo della rete
D. Un commutatore di pacchetto usato nel nucleo della rete

Answer: D
Section: AUTOVALUTAZIONE

Q636. Un accesso residenziale ad Internet di tipo FTTH (Fiber To The Home) utilizza:
A. La rete analogica telefonica per trasmettere dati digitali convertiti in formato analogico mediante un modem
B. La rete in fibra ottica fino all abitazione dell utente per trasmettere dati digitali convertiti in segnali ottici mediante un terminale ottico detto ONT (Optical Network Terminator)
C. La rete della televisione via cavo per trasmettere dati digitali convertiti mediante un cable modem
D. La rete satellitare della telefonia cellulare

Answer: B
Section: AUTOVALUTAZIONE

Q638. In PGP, la chiave simmetrica è trasferita usando:
A. La cifratura simmetrica
B. La cifratura asimmetrica
C. Non viene trasferita
D. Hash SHA-1

Answer: B
Section: AUTOVALUTAZIONE

Q638. I programmi traceroute forniscono:
A. Tutti i possibili percorsi dalla sorgente alla destinazione con l'elenco degli indirizzi IP dei router attraversati e degli ISP cui appartengono
B. Gli indirizzi IP dei router attraversati nella trasmissione di un pacchetto da una sorgente ad una destinazione con i tempi impiegati dal pacchetto per coprire il percorso di andata e ritorno da ogni router, ripetendo la trasmissione in tre prove.
C. Tutti i possibili percorsi dalla sorgente alla destinazione con i tempi totali per trasmettere un pacchetto dalla sorgente alla destinazione su ogni percorso.
D. I collegamenti in uscita da un router con le relative velocità di trasmissione

Answer: B
Section: AUTOVALUTAZIONE

Q639. Mediante il protocollo IPSec si può:
A. Crittografare e/o autenticare il traffico a livello IP
B. Distribuire chiavi crittografiche
C. Firmare documenti

D. Crittografare e/o autenticare il traffico a livello applicazione

Answer: A
Section: AUTOVALUTAZIONE

Q639. In una rete a commutazione di pacchetto il ritardo di elaborazione è il tempo impiegato dal router per:
A. Calcolare il percorso che richiede il tempo più breve per la trasmissione dal sistema periferico sorgente a quello di destinazione
B. Esaminare l intestazione del pacchetto e determinare su quale collegamento di uscita dirigerlo, più altro tempo per il controllo ed eventualmente la correzione degli errori avvenuti nella trasmissione dei bit
C. Leggere tutti i bit contenuti nel pacchetto ed elaborali con un algoritmo di compressione per ottenere un pacchetto di lunghezza minore
D. Calcolare il numero di pacchetti che devono arrivare per completare la trasmissione dati tra il sistema periferico sorgente e quello destinazione.

Answer: B
Section: AUTOVALUTAZIONE

Q641. I principali protocolli del livello di applicazione del Modello TCP/IP sono:
A. Il protocollo TCP che garantisce una trasmissione affidabile tra mittente e destinatario con ritrasmissione dei pacchetti persi, il protocollo UDP che fornisce una trasmissione con possibilità di perdita di pacchetti ma più veloce
B. Il protocollo IP che gestisce l'instradamento dei pacchetti consentendo di interconnettere reti eterogenee per tecnologia, prestazioni e gestione
C. Il protocollo HTTP per il trasferimento di documenti Web, il protocollo SMTP per la posta elettronica, il protocollo FTP per il trasferimento di file tra sistemi remoti, il protocollo DNS per la conversione di indirizzi simbolici in indirizzi numerici IP
D. Il protocollo Ethernet che gestisce le trasmissioni nelle LAN

Answer: C
Section: AUTOVALUTAZIONE

Q642. La Mobile Device Forensics si occupa di:
A. Recuperare prove digitali da un hard disk
B. Recuperare prove digitali da dispositivi mobili
C. Intercettare conversazioni telefoniche
D. Intercettare un dispositivo mobile

Answer: B
Section: AUTOVALUTAZIONE

Q642. Il principale protocollo del livello di rete del Modello TCP/IP è:
A. Il protocollo Ethernet che gestisce le trasmissioni nelle LAN
B. Il protocollo HTTP per il trasferimento di documenti Web, il protocollo SMTP per la posta elettronica, il protocollo FTP per il trasferimento di file tra sistemi remoti, il protocollo DNS per la conversione di indirizzi simbolici in indirizzi numerici IP
C. Il protocollo TCP che garantisce una trasmissione affidabile tra mittente e destinatario con ritrasmissione dei pacchetti persi, il protocollo UDP che fornisce una trasmissione con possibilità di perdita di pacchetti ma più veloce
D. Il protocollo IP che gestisce l'instradamento dei pacchetti consentendo di interconnettere reti eterogenee per tecnologia, prestazioni e gestione

Answer: D

Section: AUTOVALUTAZIONE

Q643. Le due macro-aree del MM Forensics riguardano:
A. Identificazione della sorgente di acquisizione e analisi dell'autenticità di tale sorgente
B. Identificazione della qualità e dell'autenticità di un contenuto
C. Identificazione della sorgente di acquisizione e analisi dell'autenticità di un contenuto
D. Analisi dell'autenticità di un contenuto e recupero dell'originale

Answer: C
Section: AUTOVALUTAZIONE

Q645. Ogni blocco della Blockchain contiene:
A. Hash del blocco precedente e di quello attuale, le transazioni e anche l'hash di quello successivo
B. Hash del blocco precedente ma non di quello attuale
C. I dati relativi alle transazioni
D. Hash del blocco attuale

Answer: A
Section: AUTOVALUTAZIONE

Q645. La cifratura di Feistel mette in pratica i concetti di:
A. Sostituzione e confusione
B. Diffusione e sostituzione
C. Diffusione e confusione
D. Diffusione e permutazione

Answer: C
Section: AUTOVALUTAZIONE

Q646. In Blockchain, cos'è la Proof-of-Work:
A. Un problema di sicurezza
B. Un problema crittografico senza soluzione
C. Un problema crittografico computazionalmente semplice ma la cui verifica del risultato ottenuto è molto complessa
D. Un problema crittografico computazionalmente complesso ma la cui verifica del risultato ottenuto è molto semplice

Answer: D
Section: AUTOVALUTAZIONE

Q647. Nella rete Tor, la lista dei Tor relay si ottiene da:
A. Un qualsiasi Tor relay
B. I Tor relay di guardia
C. Un directory server
D. Da una CA

Answer: C
Section: AUTOVALUTAZIONE

Q647. Il vantaggio di usare la cifratura multipla sta:
A. Nell'aumentare la velocità dell'operazione di decifratura
B. Nel poter riutilizzare l'algoritmo base estendendone la sicurezza
C. Nessun vantaggio

D. Nell'aumentare la velocità dell'operazione di cifratura

Answer: B
Section: AUTOVALUTAZIONE

Q649. Nella cifratura end-to-end sono protetti:
A. I dati utente sono in chiaro ma il flusso nella rete è protetto
B. I dati utente e il loro flusso
C. Solo una parte dei dati utente
D. I dati utente ma non il loro flusso

Answer: D
Section: AUTOVALUTAZIONE

Q651. Nel caso di utilizzo della crittografia asimmetrica per la funzione di segretezza, un eventuale attaccante può riuscire a stimare:
A. La chiave pubblica del destinatario
B. Solo il messaggio in chiaro
C. Solo la chiave privata del destinatario
D. La chiave privata del destinatario e il messaggio in chiaro

Answer: D
Section: AUTOVALUTAZIONE

Q652. Con la crittografia asimmetrica si riesce a garantire autenticazione e segretezza:
A. NO
B. Sì sempre
C. Sì ma usando entrambe le coppie di chiavi del mittente e del destinatario
D. Sì ma scambiandosi le chiavi private

Answer: C
Section: AUTOVALUTAZIONE

Q652. La tecnica store and forward nella trasmissione a commutazione di pacchetto stabilisce che:
A. Il router può iniziare la trasmissione di un pacchetto solo quando ha ricevuto tutti i pacchetti in cui è stato suddiviso il messaggio
B. Il provider autorizza la trasmissione dei pacchetti ricevuti dal router
C. Il router può iniziare la trasmissione di un pacchetto solo quando lo ha completamente ricevuto
D. Il router riceva dalla sorgente la password che consente l'accesso dei pacchetti nella destinazione

Answer: C
Section: AUTOVALUTAZIONE

Q653. Quale operazione esegue il destinatario del messaggio cifrato C:
A. Cdmodn=M
B. Cemodn=M
C. Cemod(Õ(n))=M
D. (C*d)modn=M

Answer: A
Section: AUTOVALUTAZIONE

Q653. Quando il traffico relativo ad un collegamento di uscita da un router, misurato come rapporto tra il numero medio di bit ricevuti e il numero di bit inviati nell'unità di tempo, risulta maggiore di 1 si ha che:

A. Il ritardo medio di accodamento tende all'infinito poiché la lunghezza della coda di pacchetti memorizzati nel buffer di output in attesa di essere inviati cresce continuamente

B. Il ritardo medio di accodamento cresce linearmente poiché la lunghezza della coda di pacchetti memorizzati nel buffer di output in attesa di essere inviati cresce in proporzione al ritardo

C. Il ritardo medio di accodamento è limitato superiormente da un valore finito poiché la lunghezza della coda di pacchetti memorizzati nel buffer di output in attesa di essere inviati è limitata

D. Il ritardo medio di accodamento è costante poiché la lunghezza della coda di pacchetti memorizzati nel buffer di output in attesa di essere inviati è costante

Answer: A
Section: AUTOVALUTAZIONE

Q654. Lo scambio di chiavi Diffie-Hellman è reso sicuro da:

A. L'uso di una chiave molto lunga

B. L'uso della crittografia pubblica

C. La difficoltà nel calcolo dei logaritmi discreti

D. La difficoltà nel calcolo di esponenziali

Answer: C
Section: AUTOVALUTAZIONE

Q655. La funzione usata per il codice MAC è:

A. Due-a-uno

B. Uno-a-uno

C. Molti-a-uno

D. Uno-a-molti

Answer: C
Section: AUTOVALUTAZIONE

Q655. Un PoP (Point of Presence) consiste:

A. Nella possibilità per tutti gli ISP di connettersi a due o più fornitori di livello superiore mediante un collegamento ad alta velocità. Sono esclusi gli ISP di livello 1 che non pagano fornitori

B. In un gruppo di router collocati fisicamente vicini che appartiene alla rete di un ISP fornitore. L'ISP fornitore che possiede un PoP offre ai propri ISP clienti la possibilità di collegare un loro router direttamente ad un router del PoP mediante, un collegamento ad alta velocità. Gli ISP di accesso che hanno come clienti gli utenti finali non posseggono PoP.

C. In un gruppo di router collocati fisicamente vicini che consentono ad ISP di ottimizzare i costi di una connessione di tipo peering tra le loro reti. Gli ISP clienti hanno la possibilità di collegare un loro router direttamente ad un router del PoP mediante un collegamento ad alta velocità.

D. In un insieme di attrezzature e servizi che consentono ad ISP di ottimizzare i costi di una connessione di tipo peering tra le loro reti

Answer: B
Section: AUTOVALUTAZIONE

Q659. Quale dei seguenti malware non è in realtà un software:

A. Backdoor

B. Worm
C. Virus
D. Trojan

Answer: A
Section: AUTOVALUTAZIONE

Q660. Le tecniche di MM Forensics basate sui descrittori servono principalmente per individuare l'attacco di tipo:
A. Doppia compressione JPEG
B. Filtraggio mediano
C. Giustapposizione
D. Copy-move

Answer: D
Section: AUTOVALUTAZIONE

Q660. I Meccanismi di Sicurezza pervasivi sono:
A. Specifici del servizio di sicurezza
B. Specifici del livello del protocollo
C. Orientati all'autenticazione
D. Applicabili a diversi servizi di sicurezza

Answer: D
Section: AUTOVALUTAZIONE

Q663. In una trasmissione store and forward le tabelle di inoltro sono:
A. Costruite automaticamente dal computer da cui parte la trasmissione del pacchetto
B. Memorizzate in un server del provider
C. Memorizzate nel computer da cui parte la trasmissione del pacchetto
D. Costruite automaticamentem dal router sulla base di protocolli di instradamento

Answer: D
Section: AUTOVALUTAZIONE

Q664. La rete Tor è basata su:
A. Il protocollo Crowd
B. Il protocollo MIX
C. Il protocollo SSL
D. Il protocollo Diffie-Hellman

Answer: B
Section: AUTOVALUTAZIONE

Q664. Un ISP di accesso si può connettere ad ISP di livello 1:
A. Solo con connessioni ad IXP (Internet exchange Point)
B. Sia pagando il traffico ad un ISP regionale che a sua volta paga il traffico ad un fornitore di livello 1, sia direttamente all'ISP di livello 1 pagando il relativo traffico
C. Solo con connessioni a PoP (Point of Presence)
D. Solo tramite un ISP regionale

Answer: B

Section: AUTOVALUTAZIONE

Q668. La cifratura Playfair opera:
A. Sui digrammi
B. Sui trigrammi
C. Su una tabella di cifratura 6x5
D. Sulle singole lettere

Answer: A
Section: AUTOVALUTAZIONE

Q669. In RSA, qual è il legame tra il valore d e il valore e:
A. e>d
B. e*d=1mod(Õ(n))
C. e*d=1mod(n)
D. e*d=1

Answer: B
Section: AUTOVALUTAZIONE

Q669. La tecnica Rail Fence è:
A. una tecnica basata su macchine a rotazione
B. una tecnica a trasposizione
C. una tecnica a sostituzione
D. una tecnica che usa una cifratura a blocchi

Answer: B
Section: AUTOVALUTAZIONE

Q670. La funzione hash, integrata con la cifratura simmetrica, riesce a garantire:
A. La firma digitale
B. Solo l'autenticazione
C. Solo la segretezza
D. L'autenticazione e la segretezza

Answer: D
Section: AUTOVALUTAZIONE

Q670. Nella funzione di Mix columns:
A. Ogni byte generato dipende da tutti e quattro i byte in colonna
B. Ogni byte generato dipende da tutti e quattro i byte nella riga
C. Ogni colonna è elaborata insieme a quella seguente
D. L'output contiene un numero di byte superiori all'input

Answer: A
Section: AUTOVALUTAZIONE

Q671. Nella cifratura 2DES si ha che:
A. Le due chiavi sono usate in ordine inverso in cifratura e decifratura
B. Le due chiavi possono essere usate in qualsiasi ordine in cifratura e decifratura
C. Le due chiavi sono usate nello stesso ordine in cifratura e decifratura

D. Le due chiavi hanno lunghezza di 112 bit

Answer: A
Section: AUTOVALUTAZIONE

Q673. Nella modalità Cipher Feedback il testo in chiaro è in XOR con:
A. Con il vettore di inizializzazione
B. Con il testo cifrato al passo precedente
C. Con gli s bit più significativi del testo in uscita dalla cifratura
D. Con gli s bit meno significativi del testo in uscita dalla cifratura

Answer: C
Section: AUTOVALUTAZIONE

Q674. Nell'algoritmo HMAC, l'uscita del primo hash viene:
A. Non viene estesa
B. Estesa da n (lunghezza del digest) a b bit (lunghezza del blocco)
C. Troncata da n (lunghezza del digest) a b bit (lunghezza del blocco)
D. Estesa da n (lunghezza del digest) a 1024 bit

Answer: B
Section: AUTOVALUTAZIONE

Q674. Nell'uso della crittografia simmetrica in un ambiente distribuito cosa è cruciale definire:
A. il punto in cui usare la crittografia
B. La lunghezza della chiave
C. La dimensione del blocco
D. La tecnica crittografica

Answer: A
Section: AUTOVALUTAZIONE

Q676. La crittografia asimmetrica nasce per risolvere il problema:
A. Della distribuzione delle chiavi e della firma digitale
B. Di ridurre i tempi computazionali
C. Di aumentare la robustezza
D. Di sostituire la crittografia simmetrica

Answer: A
Section: AUTOVALUTAZIONE

Q677. Nell'attacco DDoS di tipo SYN flood si inviano pacchetti TCP/IP SYN:
A. Con indirizzo del sistema target corretto ma senza indirizzo di ritorno
B. Con indirizzo del sistema target corretto ma indirizzo di ritorno errato
C. Con indirizzo di ritorno uguale a quello del target
D. Con indirizzo del sistema target errato

Answer: B
Section: AUTOVALUTAZIONE

Q677. Nella crittografia a chiave pubblica è computazionalmente impraticabile:

A. Calcolare il testo in chiaro dal testo cifrato
B. Ricavare la chiave privata da quella pubblica
C. Calcolare il testo cifrato da quello in chiaro
D. Ricavare la chiave pubblica da quella privata

Answer: B
Section: AUTOVALUTAZIONE

Q678. Il fingerprint di una fotocamera si ottiene:
A. Attraverso un'operazione di stima estraendo i PRNU da un'immagine scattata dalla fotocamera stessa
B. Attraverso un'operazione di filtraggio del PRNU
C. Attraverso un'operazione di stima estraendo i PRNU da alcune immagini scattate dalla fotocamera stessa
D. Attraverso un'operazione di stima estraendo i PRNU da alcune immagini

Answer: C
Section: AUTOVALUTAZIONE

Q680. In Blockchain, in cosa consiste la Proof-of-Work:
A. Trovare un nonce
B. Trovare un nonce tale che l'hash del nonce stesso e di altri dati produca un codice hash con caratteristiche specifiche
C. Trovare un nonce tale che l'hash di altri dati produca un codice hash con caratteristiche specifiche
D. Trovare un nonce le cui cifre iniziali siano degli 0

Answer: B
Section: AUTOVALUTAZIONE

Q680. Nel caso di funzione hash basata sullo XOR di blocchi di messaggio da 3 bit ciascuno, se un attaccante ha intercettato un hash H=010 quale dei seguenti falsi messaggi M' (da due blocchi) può inviare affinché M' sia accettato come valido rispetto a tale hash H:
A. M=[111; 000]
B. M=[111; 110]
C. M=[111; 101]
D. M=[101; 001]

Answer: C
Section: AUTOVALUTAZIONE

Q680. Internet è:
A. Un insieme di servizi quali navigazione nel Word Wide Web, posta elettronica, videoconferenze, ecc., disponibili per tutti o per una parte selezionata di utenti
B. Un sistema Software complesso che permette agli utenti lo scambio di informazioni e la condivisione di risorse e servizi
C. L'insieme degli ISP che permettono agli utenti lo scambio di informazioni e la condivisione di risorse e servizi
D. Una specifica rete pubblica che interconnette miliardi di dispositivi distribuiti in tutto il mondo offrendo all utente una vasta serie di servizi

Answer: D
Section: AUTOVALUTAZIONE

Q681. Nella rete Tor, i Tor relay di guardia servono a:
A. Non hanno compiti particolari

B. Impedire ad un attaccante di connettersi alla rete Tor
C. Impedire ad un attaccante di diventare un relay del circuito
D. Impedire ad un attaccante di diventare il primo relay del circuito

Answer: D
Section: AUTOVALUTAZIONE

Q681. Un commutatore a livello di collegamento (link-layer switch) è:
A. Un sistema periferico che scambia messaggi suddivisi in pacchetti con un dispositivo nel nucleo della rete
B. Un host che scambia messaggi suddivisi in pacchetti con un dispositivo remoto connesso in rete
C. Un commutatore di pacchetto usato nelle reti di accesso
D. Un commutatore di pacchetto usato nel nucleo della rete

Answer: C
Section: AUTOVALUTAZIONE

Q682. In Kerberos V4, la risposta dell'AS alla richiesta del client contiene fondamentalmente:
A. La chiave Kc,tgs
B. La chiave Kc,tgs e il Tickettgs
C. La chiave Kc
D. Il Tickettgs

Answer: B
Section: AUTOVALUTAZIONE

Q682. In una rete di accesso a Internet DSL la linea telefonica in uscita dall'abitazione collega lo splitter:
A. Al router del provider che gestisce la connessione
B. Al server del provider che gestisce la connessione
C. Al dispositivo detto OLT (Optica Line Terminator) che si trova nella centrale locale della compagnia telefonica
D. Al dispositivo detto DSLAM (Digital Subscriber Line Access Multiplexer) che si trova nella centrale locale della compagnia telefonica

Answer: D
Section: AUTOVALUTAZIONE

Q683. In Internet i sistemi periferici utilizzano la tecnica di trasmissione:
A. FTTH (Fiber To The Home)
B. A commutazione di circuito
C. DSL (Digital Subscriber Line)
D. A commutazione di pacchetto

Answer: D
Section: AUTOVALUTAZIONE

Q684. In IPSec, nella modalità tunnel, si fornisce protezione a:
A. L'intestazione IP
B. Il payload IP
C. L'intero pacchetto IP
D. Ad alcune parti dell'intestazione

Answer: C

Section: AUTOVALUTAZIONE

Q686. Nello standard SET la segretezza del pagamento e dell'ordine è garantita tramite:
A. Cifratura RSA
B. Hash SHA-1
C. Cifratura simmetrica DES
D. Cifratura a chiave pubblica.

Answer: C
Section: AUTOVALUTAZIONE

Q686. Considerando solo il ritardo di trasmissione nella rete in figura dove Rs bps ed Rc bps sono, rispettivamente, le velocità di trasmissione dei collegamenti server-router e router-client, il throughput medio end-to-end di una trasmissione di dati tra client e server è approssimato da:
A. Throughput medio end-to-end = (Rs+Rc)/2 bps
B. Throughput medio end-to-end = massimo(Rs, Rc) bps
C. Throughput medio end-to-end = Rs/Rc bps
D. Throughput medio end-to-end = minimo(Rs, Rc) bps

Answer: D
Section: AUTOVALUTAZIONE

Q687. Nella Purchase Request dello standard SET, il cliente invia:
A. Una chiave simmetrica monouso cifrata con la chiave pubblica del venditore
B. Una chiave simmetrica monouso cifrata con la chiave pubblica del gateway di pagamento
C. Una chiave simmetrica monouso non cifrata
D. Una chiave simmetrica monouso cifrata con un hash

Answer: B
Section: AUTOVALUTAZIONE

Q687. Considerando solo il ritardo di trasmissione nella rete in figura, quando attraverso il collegamento comune di velocità R nel nucleo della rete, condiviso ad intervalli di tempo uguali, avvengono 10 trasmissioni di dati contemporane tra 10 coppie client-server , se la velocità del collegamento comune disponibile per ogni trasferimento dati rimane superiore alle velocità di accesso al nucleo della rete Rc dei client ed Rs dei server, il throughput medio end-to-end di una trasmissione di dati tra una coppia client-server è approssimato da:
A. Throughput medio end-to-end = R bps
B. Throughput medio end-to-end = massimo(Rs,Rc) bps
C. Throughput medio end-to-end = minimo(Rs, Rc) bps
D. Throughput medio end-to-end =(Rs+Rc)/2 bps

Answer: C
Section: AUTOVALUTAZIONE

Q689. La rete di un ISP di livello 1 si connette a Internet:
A. Solo con connessioni ad IXP (Internet exchange Point)
B. Solo con connessione di tipo peering
C. Solo con connessioni ad PoP (Point of Presence)
D. Solo con modalità multi-homing

Answer: B

Section: AUTOVALUTAZIONE

Q690. Le tecniche di MM Forensics, basate sull'analisi delle traiettorie degli oggetti, sono utilizzate per:
A. Determinare se il formato di codifica di una sequenza video è stato manipolato
B. Determinare se un'immagine è manipolata
C. Non esistono tecniche di questo tipo
D. Determinare se una sequenza video è manipolata

Answer: D
Section: AUTOVALUTAZIONE

Q690. Il livello Fisico dello standard ISO/OSI offre servizi:
A. Che permettono un trasferimento di dati affidabile, effettuando anche un controllo degli errori e delle perdite di pacchetti tra due sistemi periferici
B. Per il trasferimento di dati tra nodi adiacenti attraverso il tipo di collegamento che sussiste tra di loro
C. Necessari a livello Hardware per controllare il flusso di dati attraverso i collegamenti e le connessioni ai dispositivi che permettono il passaggio dei segnali che rappresentano le informazioni
D. Che consentono la comunicazione tra i nodi della rete che vengono attraversati nel percorso che va dal sistema periferico sorgente al sistema periferico destinazione

Answer: C
Section: AUTOVALUTAZIONE

Q691. In una rete a commutazione di pacchetto basata sull'Architettura a livelli l'header è:
A. Il livello più alto nella gerarchia definita dal Modello standard ISO/OSI
B. Il campo del pacchetto relativo ad un livello, che contiene il pacchetto gestito dal livello superiore
C. Il campo del pacchetto relativo ad un livello, che contiene le informazioni aggiuntive gestite dai protocolli di tale livello
D. Il livello più alto nella gerarchia definita dal Modello standard TCP/IP

Answer: C
Section: AUTOVALUTAZIONE

Q692. In una transazione blockchain, i nodi della rete verificano:
A. La correttezza della transazione
B. La provenienza della richiesta
C. La PoW
D. L'hash del blocco

Answer: A
Section: AUTOVALUTAZIONE

Q692. Un malware viene detto autoreplicante quando:
A. Può diffondere in rete copie di se stesso, che effettuano lo stesso tipo di attacco su altri computer
B. Può diffondere in rete copie dei file memorizzati sul computer infettato di un utente inconsapevole
C. Può copiare sul computer dell'attaccante i i file memorizzati sul computer infettato di un utente inconsapevole
D. Può ripetere un attacco informatico ad intervalli di tempo regolari su uno stesso computer

Answer: A
Section: AUTOVALUTAZIONE

Q694. I Meccanismi di Sicurezza si dividono in:
A. Specifici e alternativi
B. Generici e pervasivi
C. Specifici e diretti
D. Specifici e pervasivi

Answer: D
Section: AUTOVALUTAZIONE

Q696. La cifratura monoalfabetica si presenta come:
A. Uguale alla cifratura di Cesare
B. La cifratura di Cesare ma con un numero di chiavi pari a 26!
C. Una cifratura inattaccabile
D. Facile da attaccare anche se non si conosce la natura del testo in chiaro

Answer: B
Section: AUTOVALUTAZIONE

Q698. Nel caso di utilizzo della crittografia asimmetrica per la funzione di autenticazione:
A. Il mittente usa in cifratura la chiave pubblica del destinatario
B. Il mittente usa in cifratura la chiave privata del destinatario
C. Il mittente usa in cifratura la propria chiave pubblica
D. Il mittente usa in cifratura la propria chiave privata

Answer: D
Section: AUTOVALUTAZIONE

Q700. Nell'algoritmo SHA-512 il digest di uscita è ottenuto:
A. Dopo aver eseguito l'elaborazione del modulo F ed effettuato la somma con l'output allo stadio precedente, per tutti gli N blocchi del messaggio
B. Dopo aver calcolato le 80 fasi
C. Dopo aver eseguito l'elaborazione del modulo F
D. Dopo aver eseguito l'elaborazione del modulo F ed effettuato la somma con l'input allo stadio precedente, per tutti gli N blocchi del messaggio

Answer: A
Section: AUTOVALUTAZIONE

Q702. Il packet sniffing è:
A. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server
B. La diffusione in rete di copie dei file memorizzati su un computer
C. La copia mediante un ricevitore passivo di ogni pacchetto in transito su una connessione all insaputa degli utenti collegati che non hanno modo per potersene accorgere
D. Un malware autoreplicante che richiede una qualche forma di interazione con l utente per poter infettare il dispositivo

Answer: C
Section: AUTOVALUTAZIONE

Q703. In IPSec, nel protocollo ESP in modalità trasporto, l'intestazione ESP si trova:

A. Prima della nuova intestazione IP
B. Dopo l'intestazione IP originaria
C. Prima dell'intestazione IP originaria
D. Dopo la nuova intestazione IP

Answer: B
Section: AUTOVALUTAZIONE

Q704. In IPSec la gestione delle chiavi si basa fondamentalmente su:
A. Protocolli Oakley e ISAKMP
B. Diffie-Hellman
C. Protocollo Oakley
D. Protocollo ISAKMP

Answer: A
Section: AUTOVALUTAZIONE

Q705. In PGP, l'autenticazione viene garantita tramite:
A. La cifratura simmetrica e l'algoritmo ZIP
B. Hash SHA-1 e la cifratura simmetrica
C. Hash SHA-1 e la cifratura asimmetrica
D. La cifratura simmetrica

Answer: C
Section: AUTOVALUTAZIONE

Q705. In ciascuna fase la parte Ri-1:
A. Va in XOR con la sottochiave Ki
B. Va in XOR con la sottochiave Ki-1
C. Dopo essere stata espansa e permutata va in XOR con la sottochiave Ki
D. Dopo essere stata espansa e permutata va in XOR con l'altra metà

Answer: C
Section: AUTOVALUTAZIONE

Q706. Il firewall è in grado di fornire anche:
A. Protezione da attacchi interni
B. Un punto di osservazione di eventi relativi alla sicurezza della rete interna
C. Nient'altro che una barriera di sicurezza
D. Protezione da documenti infettati da virus

Answer: B
Section: AUTOVALUTAZIONE

Q706. Nella funzione di Byte substitution:
A. Si esegue una permutazione ciclica
B. L'operazione si basa su una S-box composta da 64 valori
C. L'operazione si basa su una S-box composta da 256 valori
D. I primi 4 bit e i secondi 4 bit individuano rispettivamente la colonna e la riga della S-box

Answer: C

Section: AUTOVALUTAZIONE

Q709. In RSA il valore n=p*q è:
A. Pubblico e scelto dall'utente
B. Privato e scelto dall'utente
C. Pubblico e calcolato dall'utente
D. Privato e calcolato dall'utente

Answer: C
Section: AUTOVALUTAZIONE

Q711. In RSA, cosa permette di fare l'algoritmo di Euclide esteso:
A. Selezionare e o d e calcolare l'altro valore
B. Selezionare n o d e calcolare l'altro valore
C. Calcolare MCD(Õ(n),e)
D. Calcolare MCD(d,e)

Answer: A
Section: AUTOVALUTAZIONE

Q711. Una connessione di tipo peering tra reti di ISP consiste:
A. Nel pagamento da parte di un ISP del traffico fornito da un fornitore di livello superiore
B. In una connessione attraverso collegamenti ad alta velocità
C. In una connessione in cui nessuno degli ISP collegati paga l'altro per lo scambio di traffico che avviene tra le loro reti, ma ciascuno raccoglie separatamente per se stesso i pagamenti dai propri clienti
D. In una connessione diretta tramite un PoP (Point of Presence) mediante un collegamento ad alta velocità

Answer: C
Section: AUTOVALUTAZIONE

Q712. Rispetto ai modelli ISO/OSI e TCP/IP l'approccio cross-layer è:
A. Diverso perché introduce la capacità di scambiare informazioni anche tra protocolli relativi a livelli diversi
B. Uguale perché i protocolli possono comunicare solo con protocolli dello stesso livello
C. Diverso perché introduce la capacità di scambiare l'ordine gerarchico dei livelli
D. Diverso perché unifica il livello di rete con quello di collegamento

Answer: A
Section: AUTOVALUTAZIONE

Q713. La crittografia asimmetrica che usa in cifratura la chiave privata del mittente può garantire:
A. Autenticazione e segretezza
B. Segretezza ma non autenticazione
C. Autenticazione ma non segretezza
D. Né autenticazione né segretezza

Answer: C
Section: AUTOVALUTAZIONE

Q714. Quali aspetti non sono da considerare fondamentali nella progettazione di un sistema di sicurezza:
A. Gestione delle informazioni segrete
B. Analisi dei potenziali attacchi

C. Praticabilità
D. Posizione fisica del server

Answer: D
Section: AUTOVALUTAZIONE

Q715. In PGP, la conversione radix-64 determina:
A. Un aumento della dimensione del messaggio
B. Una decifratura del messaggio
C. Un rallentamento
D. Una conversione byte a byte

Answer: A
Section: AUTOVALUTAZIONE

Q715. Quali di questi attacchi non è attivo:
A. Ripetizione
B. Mascheramento
C. Denial-of-Service
D. Analisi del traffico

Answer: D
Section: AUTOVALUTAZIONE

Q716. DJBP è un testo cifrato, secondo la cifratura di Giulio Cesare, del seguente testo in chiaro:
A. CAIO
B. CIAO
C. CANE
D. CARO

Answer: B
Section: AUTOVALUTAZIONE

Q717. Quale delle seguenti affermazioni è falsa:
A. NIST richiedeva per AES l'uso di blocchi a 128 bit
B. NIST richiedeva per AES l'uso di chiavi di differente lunghezza
C. L'algoritmo Rijndael fu selezionato per AES
D. L'algoritmo Rijndael si basa sui blocchi di Feistel

Answer: D
Section: AUTOVALUTAZIONE

Q718. In SSL, il protocollo Alert specifica:
A. Il livello di severità dell'alert e la sua tipologia
B. Il livello di severità dell'alert
C. Invia un alert
D. La tipologia di alert

Answer: A
Section: AUTOVALUTAZIONE

Q718. Nella funzione di Add round key:
A. Viene eseguita una espansione della chiave
B. Si esegue un'operazione di XOR bit a bit tra il testo e la chiave seguita da una permutazione ciclica
C. Si esegue un'operazione di XOR bit a bit tra il testo e la chiave
D. Si esegue un'operazione di XOR bit a bit tra il testo e la chiave ma la chiave ha lunghezza diversa nelle varie fasi

Answer: C
Section: AUTOVALUTAZIONE

Q721. Quale dei seguenti non è un malware vero e proprio:
A. Worm
B. Spyware
C. Backdoor
D. Trojan

Answer: C
Section: AUTOVALUTAZIONE

Q721. Nella crittografia end-to-end se ci sono N host che devono scambiarsi dati, quante chiavi sono necessarie:
A. N
B. N/2
C. [N(N-1)]/2
D. N(N-1)

Answer: C
Section: AUTOVALUTAZIONE

Q724. Il rumore PRNU è generato da:
A. Il rumore di acquisizione
B. Una risposta differente dei CCD all intensità di luce
C. Dal malfunzionamento dei CCD rispetto all intensità di luce
D. Dal deterioramento nel tempo dei CCD

Answer: B
Section: AUTOVALUTAZIONE

Q725. Il vantaggio della modulatità offerto dalla Architettura a livelli consiste nella possibilità di:
A. Cambiare un host periferico senza dover cambiare l implementazione della parte rimanente del sistema
B. Aggiungere un numero non limitato di dispositivi periferici connessi in rete
C. Scegliere più ISP (Internet Service Provider) per collegarsi alla rete
D. Cambiare l implementazione dei servizi forniti dal protocollo di un particolare livello senza dover cambiare l implementazione della parte rimanente del sistema

Answer: D
Section: AUTOVALUTAZIONE

Q726. Nell'algoritmo HMAC, la chiave K+ viene ricavata a partire dalla chiave K:
A. Attraverso un'operazione di riempimento a sinistra con una serie di 0 fino ad avere lunghezza uguale a quello del blocco
B. Attraverso un'operazione di riempimento a sinistra con una serie di 1 fino ad avere lunghezza uguale a quello del blocco

C. Attraverso un'operazione di troncamento pari alla lunghezza del blocco
D. Attraverso un'operazione di XOR con il valore ipad oppure opad

Answer: A
Section: AUTOVALUTAZIONE

Q727. L'algortimo CMAC usa come cifratura:
A. DES e AES
B. DES o AES
C. Solo DES
D. RSA

Answer: B
Section: AUTOVALUTAZIONE

Q727. La suite di protocolli TCP/IP è:
A. Il Modello della pila di protocolli implementati in Internet definita da 4 protocolli nello standard RFC 1122 del 1989
B. Il Modello della pila di protocolli implementati in Internet definita da 4 livelli nello standard RFC 1122 del 1989
C. Il Modello della pila di protocolli di rete definita da 7 protocolli nello standard del 1984
D. Il Modello della pila di protocolli di rete definita da 7 livelli nello standard del 1984

Answer: B
Section: AUTOVALUTAZIONE

Q728. In Kerberos V4, il Tickettgs è cifrato con:
A. La chiave segreta del server TGS
B. La chiave pubblica del server TGS
C. La chiave privata del client
D. La chiave Kc,tgs

Answer: A
Section: AUTOVALUTAZIONE

Q729. Nel caso di accesso host da remoto verso un server posto all'interno di una rete aziendale, quale di queste combinazione di SA appare più adatta:
A. Una SA di tipo trasporto
B. Una SA di tipo trasporto fra host e gateway della rete con una o due SA fra gateway e server
C. Una SA di tipo tunnel fra host e gateway della rete con una o due SA fra gateway e server
D. Una SA di tipo tunnel fra host e gateway della rete con una o due SA fra host e server

Answer: D
Section: AUTOVALUTAZIONE

Q730. In IPSec, nel protocollo AH, la finestra anti-replay consente di:
A. Scartare i pacchetti non validi
B. Scartare i pacchetti con valore a sinistra della finestra anche se validi
C. Scartare i pacchetti con valore a sinistra della finestra se non validi
D. Scartare i pacchetti con valore a destra della finestra anche se validi

Answer: B
Section: AUTOVALUTAZIONE

Q732. A cosa è dovuta la traccia relativa alla distorsione della lente:
A. Alla distorsione radiale indotta dal fatto che la lente non è ideale
B. Alla successiva compressione JPEG
C. Alla distorsione radiale indotta dal filtro ottico
D. Alla distorsione radiale indotta dal CFA

Answer: A
Section: AUTOVALUTAZIONE

Q733. Nella crittografia asimmetrica l'operazione Y=fk(X) deve essere:
A. Facile se X noto
B. Difficile da calcolare
C. Facile se X e K noti
D. Non invertibile

Answer: C
Section: AUTOVALUTAZIONE

Q734. In Blockchain, cosa rappresenta il nonce:
A. Un numero casuale
B. Il numero soluzione della PoW
C. La chiave dell'hash
D. L'uscita dell'hash

Answer: B
Section: AUTOVALUTAZIONE

Q737. Nella rete Tor, i "servizi nascosti" sono:
A. Servizi web a cui non si riesce ad accedere
B. Servizi di cui non è visibile l'indirizzo IP
C. Servizi web non legittimi
D. Servizi a cui si accede solo dopo una registrazione specifica

Answer: B
Section: AUTOVALUTAZIONE

Q741. I server di autenticazione svolgono la funzione di:
A. Garantire i server
B. Garantire utenti e server
C. Garantire gli utenti
D. Garantire l'integrità dei dati

Answer: B
Section: AUTOVALUTAZIONE

Q743. La crittografia simmetrica può garantire:
A. La firma digitale
B. Segretezza e autenticazione
C. Non ripudiabilità
D. Da sola non dà garanzia

Answer: B
Section: AUTOVALUTAZIONE

Q743. In una trasmissione store and forward un pacchetto ricevuto da un router che non può essere trasmesso perché il collegamento in uscita non è disponibile viene:
A. Memorizzato e messo in coda in attesa della trasmissione nel buffer di output del computer che invia il messaggio
B. Memorizzato e messo in coda in attesa della trasmissione nel buffer di output del router
C. Memorizzato e messo in coda in attesa della trasmissione nel buffer di output del provider
D. Memorizzato e messo in coda in attesa della trasmissione in un server del provider

Answer: B
Section: AUTOVALUTAZIONE

Q745. In quale modo un worm decide come propagarsi:
A. Sceglie prima le macchine vicine geograficamente
B. Sulla base delle vulnerabilità
C. Sulla base di una temporizzazione
D. Scansionando la rete sulla base di criteri predefiniti dall'hacker

Answer: D
Section: AUTOVALUTAZIONE

Q745. Un codice MAC è caratterizzato da una funzione del tipo:
A. MAC=C(M)
B. MAC=C(K||M)
C. MAC=C(K,M)
D. MAC=C(K, XOR(K,M))

Answer: C
Section: AUTOVALUTAZIONE

Q746. L'algoritmo SHA-512 prevede di usare dei bit di riempimento per adattare:
A. La lunghezza del messaggio ad un numero di blocchi multiplo di 512
B. La lunghezza del messaggio ad un numero di blocchi multiplo di 1024
C. Il numero di blocchi da elaborare
D. La lunghezza del digest di output

Answer: B
Section: AUTOVALUTAZIONE

Q747. Cosa si ntende con il termine "demosaicking":
A. Un'operazione di esaltazione di valori di colore
B. Un'operazione di eliminazione di valori di colore
C. Un'operazione di generazione di valori di colore
D. Un'operazione di combinazione di valori di colore

Answer: C
Section: AUTOVALUTAZIONE

Q748. Con il termine "intrusione" si intende:

A. Un accesso non consentito ad un server
B. Un accesso non consentito ad un sistema e alla informazioni in esso contenute
C. Un accesso non consentito ad una applicazione
D. Un accesso non consentito ad un documento

Answer: B
Section: AUTOVALUTAZIONE

Q748. Un attaccante tenta di accedere all'account di posta di un altro utente, si tratta di un attacco di:
A. Mascheramento
B. Denial-of-Service
C. Intercettazione
D. Modifica dei messaggi

Answer: A
Section: AUTOVALUTAZIONE

Q749. Dato K=1101 e P=1101 determinare il testo cifrato:
A. Il testo cifrato è 0000
B. Il testo cifrato è 0001
C. Il testo cifrato è 1000
D. Il testo cifrato è 1111

Answer: A
Section: AUTOVALUTAZIONE

Q750. Nel caso di attacchi di Adversarial Machine Learning, l'attaccante ha lo scopo di:
A. Indurre in errore il classificatore, basato su ML, attraverso la generazione di un'immagine compressa due volte
B. Inibire il classificatore, basato su ML, attraverso una serie di richieste
C. Indurre in errore il classificatore, basato su ML, attraverso una modifica dell'immagine
D. Indurre in errore il classificatore, basato su ML, mantenendo percettivamente minima la modifica apportata all'immagine di ingresso

Answer: D
Section: AUTOVALUTAZIONE

Q750. Quale affermazione è sbagliata:
A. Le macchine a rotazione effettuano una cifratura a flusso
B. Nelle macchine a rotazione il numero di cilindri determina la complessità della cifratura
C. Nelle macchine a rotazione l'input di una cifra non determina un cambiamento di stato della macchina
D. Nelle macchine a rotazione ogni cilindro ha 26 terminali di ingresso e 26 di uscita

Answer: C
Section: AUTOVALUTAZIONE

Q751. Il certificato X.509 contiene:
A. Le chiavi privata e pubblica del possessore del certificato
B. La chiave pubblica del possessore del certificato
C. La chiave privata del possessore del certificato
D. La chiave pubblica della CA

Answer: B
Section: AUTOVALUTAZIONE

Q752. Nel protocollo Mix, il messaggio del mittente verso il destinatario è cifrato con:
A. Le chiavi private dei proxy da cui deve transitare
B. La chiave pubblica del primo proxy
C. Le chiavi pubbliche dei proxy da cui deve transitare
D. La chiave pubblica dell'ultimo proxy

Answer: C
Section: AUTOVALUTAZIONE

Q752. In un certificato X.509, esistono sostanzialmente due parti:
A. La parte non firmata e la parte firmata dalla CA
B. La parte pubblica e la parte privata
C. La parte non firmata e la parte firmata dal possessore del certificato
D. La parte non firmata e la parte per la chiave pubblica

Answer: A
Section: AUTOVALUTAZIONE

Q753. In IPSec, il protocollo Oakley permette di difendersi dagli attacchi replay tramite:
A. Cifratura RSA
B. L'uso di nonce
C. Modalità tunnel
D. Non permette di difendersi da attacchi replay

Answer: B
Section: AUTOVALUTAZIONE

Q754. Il protocollo SSL, nell'ambito dello stack dei protocolli TCP/IP, opera:
A. A livello IP
B. Sotto al livello TCP
C. Sopra al livello TCP
D. Allo stesso livello di IPSec

Answer: C
Section: AUTOVALUTAZIONE

Q755. Con il termine "effetto valanga" si intende.
A. L'aumento di complessità di un algoritmo di crittografia
B. Testi in chiaro che differiscono di pochi bit sono codificati in testi cifrati molto diversi fra loro seppur codificati con la stessa chiave
C. Testi in chiaro che differiscono di pochi bit sono codificati in testi cifrati molto diversi fra loro se codificati con una chiave diversa
D. Testi in chiaro identici sono codificati in testi cifrati molto diversi fra loro seppur codificati con la stessa chiave

Answer: B
Section: AUTOVALUTAZIONE

Q757. Nello standard SET, la doppia firma DS è ottenuta:

A. E(PRC,H[H(PI)||H(OI)])
B. E(PRC,H(PI))
C. E(PRC,H(OI))
D. H[H(PI)||H(OI)]

Answer: A
Section: AUTOVALUTAZIONE

Q757. Una rete privata di un grande distributore di contenuti come Google può connettersi:
A. Anche alle reti di ISP di livello basso tramite connessioni a PoP (Point of Presence) pagando il traffico dei dati
B. Anche alle reti di ISP di livello basso con collegamenti di tipo peering sia direttamente sia tramite connessioni a IXP (Internet exchange Point)
C. Anche alle reti di ISP di livello basso con modalità multi-homing
D. Anche alle reti di ISP di livello basso tramite un servizio di housing (colocation)

Answer: B
Section: AUTOVALUTAZIONE

Q758. La Bomba Logica costituisce nello specifico:
A. Un malware che si propaga tramite la posta elettronica
B. Un virus indipendente
C. Un attacco informatico
D. Il codice incorporato in un malware e programmato per attivarsi

Answer: D
Section: AUTOVALUTAZIONE

Q758. L'algoritmo SHA-512 utilizza un buffer a 8 registri che serve per:
A. Appoggiare l'elaborazione di ogni fase
B. Solo per l'inizializzazione
C. Memorizzare le costanti
D. Il digest di uscita

Answer: A
Section: AUTOVALUTAZIONE

Q758. Il livello di Collegamento dello standard ISO/OSI offre servizi:
A. Necessari a livello Hardware per controllare il flusso di dati attraverso i collegamenti e le connessioni ai dispositivi che permettono il passaggio dei segnali che rappresentano le informazioni
B. Per il trasferimento di dati tra nodi adiacenti attraverso il tipo di collegamento che sussiste tra di loro
C. Che permettono un trasferimento di dati affidabile, effettuando anche un controllo degli errori e delle perdite di pacchetti tra due sistemi periferici
D. Che consentono la comunicazione tra i nodi della rete che vengono attraversati nel percorso che va dal sistema periferico sorgente al sistema periferico destinazione

Answer: B
Section: AUTOVALUTAZIONE

Q759. Nella CRL dei certificati X.509 quale dei seguenti campi non è presente:
A. La data di creazione della lista
B. La data del prossimo aggiornamento della lista

C. Il nome dell'autorità che ha emesso la CRL
D. La data in cui il certificato sarà di nuovo valido

Answer: D
Section: AUTOVALUTAZIONE

Q761. Nel PGP la compatibilità con le funzionalità di posta elettronica sono garantite attraverso:
A. L'algoritmo ZIP
B. La decifratura simmetrica
C. La conversione ASCII radix-64
D. La decifratura asimmetrica

Answer: C
Section: AUTOVALUTAZIONE

Q762. Il servizio di controllo degli accessi definisce:
A. chi può avere accesso a una risorsa, in quali condizioni può farlo e cosa può farne
B. Come impedire gli accessi
C. Quanti utenti possono accedere
D. La politica di invio dei dati

Answer: A
Section: AUTOVALUTAZIONE

Q763. In IPSec, gli extension header possono identificare i protocolli:
A. AH o ESP
B. Solo AH
C. Solo ESP
D. Non identificano nessun protocollo

Answer: A
Section: AUTOVALUTAZIONE

Q763. In una trasmissione store and forward il tempo di trasmissione di N pacchetti di L bit da una sorgente ad una destinazione entrambe connesse ad un router da collegamenti con velocità di trasmissione R bps è:
A. (N+1)(2L-R) secondi
B. (N+1)2L/R secondi
C. (N+1)L/R secondi
D. (N+1)(L-R) secondi

Answer: C
Section: AUTOVALUTAZIONE

Q764. Nel protocollo TLS, la funzione pseudo-random ha l'obiettivo di:
A. Generare numeri pseudo-casuali
B. Comprimere i valori segreti in una serie di blocchi di dati sicuri
C. Espandere i valori segreti in una serie di blocchi di dati sicuri
D. Generare un codice MAC

Answer: C
Section: AUTOVALUTAZIONE

Q765. Nello standard SET, il venditore dialoga:
A. Solo con il cliente
B. Solo con la banca del cliente
C. Con il cliente e il gateway di pagamento
D. Solo con il gateway di pagamento

Answer: C
Section: AUTOVALUTAZIONE

Q766. Quale delle seguenti modalità di distribuzione della chiave segreta non è praticabile:
A. A consegna fisicamente la chiave a B
B. Un KDC consegna fisicamente la chiave ad A e B
C. A sceglie una chiave e la invia a B
D. A e B possiedono già una chiave condivisa e usano quella per scambiarsene una nuova

Answer: C
Section: AUTOVALUTAZIONE

Q767. Esistono tecniche di MM Forensics che permettono di:
A. Determinare la sorgente di acquisizione che ha generato un determinato documento multimediale
B. Determinare la sorgente di acquisizione di un determinato documento multimediale ma non se in formato compresso
C. Determinare l'utente che ha acquisito un determinato contenuto multimediale
D. Determinare informazioni sugli utenti che sono in possesso di un determinato contenuto multimediale

Answer: A
Section: AUTOVALUTAZIONE

Q769. I "miner" sono:
A. Nodi di attacco alla blockchain
B. Nodi della rete P2P
C. Nodi specifici della rete P2P che si occupano aggiornare il Ledger
D. Nodi specifici della rete P2P che si occupano di risolvere le PoW

Answer: D
Section: AUTOVALUTAZIONE

Q771. Il Deep Web è accessibile tramite:
A. Un comune browser
B. La rete Tor
C. La cifratura asimmetrica
D. Un portale protetto

Answer: B
Section: AUTOVALUTAZIONE

Q771. In una Rete di calcolatori i sistemi periferici, detti anche host, sono:
A. Solo i computer e gli smartphone collegati in rete con l'esclusione di altre tipologie come sensori, elettrodomestici, smart TV, ecc.
B. Tutti i dispositivi collegati in rete con l'esclusione degli smartphone

C. Tutti i dispositivi collegati in rete di qualunque tipologia
D. Solo gli smartphone collegati in rete

Answer: C
Section: AUTOVALUTAZIONE

Q772. L'espansione della chiave:
A. Espande la chiave da 4 word a 44 word
B. Esegue solo delle operazioni di XOR
C. Espande la chiave da 4 word a 16 word
D. Espande la chiave da 4 word a 44 word ma non tutte vengono poi adoperate

Answer: A
Section: AUTOVALUTAZIONE

Q772. In una rete di accesso a Internet FTTH il dispositivo OLT (Optical Line Terminator) effettua:
A. La conversione tra segnali ottici e segnali elettrici digitali nella centrale locale della compania telefonica e consente il collegamento ad Internet tramite un router del provider
B. La conversione tra segnali ottici e segnali elettrici digitali nell'abitazione dell'utente
C. Il collegamento finale tra il sistema periferico e l'edge router
D. Il collegamento finale tra il sistema periferico e il server del provider che gestisce la connessione

Answer: A
Section: AUTOVALUTAZIONE

Q773. Il protocollo Kerberos V4, in una autenticazione client-server, si basa su:
A. Tanti server di autenticazione distribuiti
B. Un server di autenticazione centralizzato
C. Due server di autenticazione centralizzati
D. Nessun server di autenticazione

Answer: C
Section: AUTOVALUTAZIONE

Q774. Considerando solo il ritardo di trasmissione nella rete in figura dove Rs bps ed Rc bps sono, rispettivamente, le velocità dei collegamenti di accesso al nucleo della rete del server e del client, se tutti i collegamenti presenti nel nucleo della rete hanno velocità di trasmissione molto alta e molto più grande rispetto alle velocità dei collegamenti di accesso al nucleo della rete del server e del client, il throughput medio end-to-end di una trasmissione di dati tra client e server è approssimato da:
A. Throughput medio end-to-end = (Rs+Rc)/2 bps
B. Throughput medio end-to-end = massimo(Rs,Rc) bps
C. Throughput medio end-to-end = Rs/Rc bps
D. Throughput medio end-to-end = minimo(Rs, Rc) bps

Answer: D
Section: AUTOVALUTAZIONE

Q775. La crittografia asimmetrica è vulnerabile a:
A. Solo ad attacchi ad analisi del traffico
B. Non è vulnerabile
C. Attacchi a forza bruta

D. Solo ad attacchi che stimano la chiave privata

Answer: C
Section: AUTOVALUTAZIONE

Q775. Un servizio di housing (colocation) consiste:
A. Nel collegamento tra due sistemi periferici tramite ruters che appartengono a reti di ISP dello stesso livello gerarchico
B. Nella possibilità per tutti gli ISP di connettersi a due o più fornitori di livello superiore. Sono esclusi gli ISP di livello 1 che non pagano fornitori
C. Nel realizzare una connessione di tipo peering tra due ISP mediante le attrezzature di un ISP di livello gerarchico superiore che garantisce la gestione degli aspetti hardware, software ed infrastrutturali come il condizionamento termico e la vigilanza
D. Nel concedere in affitto uno spazio fisico in un Data center (generalmente all'interno di appositi armadi detti rack) dove posizionare i router di proprietà dell ISP che fruisce del servizio. Il Data center garantisce la gestione degli aspetti hardware, software ed infrastrutturali come il condizionamento termico e la vigilanza

Answer: D
Section: AUTOVALUTAZIONE

Q778. Negli algoritmi hash di tipologia SHA, esiste un limite sulla lunghezza del messsaggio in ingresso:
A. No non esiste
B. Sì, devono essere multipli di 1024
C. Sì, devono essere multipli di 512
D. Sì, devono essere minori di 264 o 2128 dipende dalle versioni

Answer: D
Section: AUTOVALUTAZIONE

Q778. Quando un sistema è sottoposto ad un attacco passivo:
A. Il destinatario dei messaggi non riceve niente
B. Il mittente dei messaggi capisce che la trasmissione non va a buon fine
C. I messaggi sono inviati e ricevuti in maniera apparentemente normale
D. Il destinatario si accorge che qualcuno sta ascoltando la trasmissione

Answer: C
Section: AUTOVALUTAZIONE

Q780. Nell'algoritmo HMAC, i valori ipad e opad servono per:
A. Invertire lo stato dei bit della chiave
B. Invertire lo stato di metà dei bit della chiave
C. Mettere a 1 lo stato dei bit della chiave
D. Mettere a 0 lo stato dei bit della chiave

Answer: B
Section: AUTOVALUTAZIONE

Q781. Un attacco DDoS cerca di minare:
A. Le risorse interne di un server e/o le risorse di rete verso un certo servizio
B. Le risorse interne di un server ma non le risorse di rete verso un certo servizio
C. L'accesso di un utente verso un certo servizio

D. I file system di più sistemi interconnessi

Answer: A
Section: AUTOVALUTAZIONE

Q781. Indicare quale relazione implicherebbe la riduzione ad una sola fase nel 2DES:
A. E(K2,E(K1,P))=E(K1,P)
B. E(K2,E(K1,P))=E(K3,P)
C. D(K2,E(K1,P))=E(K3,P)
D. E(K2,E(K1,P))=C

Answer: B
Section: AUTOVALUTAZIONE

Q782. In RSA , a quanto equivale Õ(n):
A. p*q
B. (p-1)*(q-1)
C. p*(q-1)
D. (p+1)*(q+1)

Answer: B
Section: AUTOVALUTAZIONE

Q783. In quali casi un certificato X.509 non finisce in CRL (Certificate Revocation List)
A. Certificato scaduto
B. La chiave privata dell'utente è stata violata
C. L'utente non è più certificato da quella CA
D. Il certificato è stato violato

Answer: A
Section: AUTOVALUTAZIONE

Q784. PGP è uno standard per la posta elettronica basata su:
A. Cifratura RSA
B. Hash SHA-1
C. Cifratura simmetrica 3DES
D. Cifratura pubblica, cifratura simmetrica e hash.

Answer: D
Section: AUTOVALUTAZIONE

Q784. Le regole che governano la comunicazione in Internet tra due o più entità remote sono stabilite da:
A. Un programma Software in esecuzione sui sistemi periferici che sono in comunicazione
B. L'invio di messaggi da parte dell'Internet Service Provider (ISP) per gestire il traffico delle trasmissioni
C. Protocolli standard specifici per le varie operazioni da svolgere
D. Una parte dell'Hardware installato sui sistemi periferici che sono in comunicazione

Answer: C
Section: AUTOVALUTAZIONE

Q785. L'algoritmo SHA-512 prende in input:

A. Blocchi di messaggio di 1024 bit
B. Blocchi di messaggio di 512 bit
C. Blocchi di messaggio di 256 bit
D. Blocchi di messaggio di dimensione variabili

Answer: A
Section: AUTOVALUTAZIONE

Q785. In una rete a commutazione di pacchetto il ritardo di propagazione relativo ad un collegamento in uscita di un router è il tempo:
A. Impiegato dal router per instradare il pacchetto verso il collegamento, dato dal valore del rapporto L/R, dove L è la lunghezza in bit del pacchetto ed R è la velocità di trasmissione in bit per secondi del collegamento in uscita del router
B. Che un segnale impiega per percorrere il collegamento dato dal valore del rapporto d/v, dove d è la lunghezza in metri del collegamento che il pacchetto in uscita dal router deve percorrere per giungere al nodo successivo della rete, e v è la velocità in metri al secondo con cui viaggia il segnale caratteristica del materiale di cui è fatto il collegamento
C. Impiegato dal router per esaminare l intestazione del pacchetto e determinare su quale collegamento di uscita dirigerlo, più altro tempo eventuale per il controllo degli errori avvenuti nella trasmissione dei bit
D. Che un pacchetto impiega per raggiungere il sistema periferico di destinazione

Answer: B
Section: AUTOVALUTAZIONE

Q786. In SSL, quale delle seguenti non è una fase del protocollo Handshake :
A. Autenticazione del server e scambio delle chiavi
B. Inizializzazione delle funzionalità di sicurezza
C. Autenticazione del client e scambio delle chiavi
D. Autenticazione del client presso la CA

Answer: D
Section: AUTOVALUTAZIONE

Q791. Nel protocollo Mix, ogni proxy possiede:
A. Una coppia di chiavi pubblica/privata
B. Una chiave segreta
C. La chiave pubblica del proxy con cui deve comunicare
D. La chiave pubblica del mittente

Answer: A
Section: AUTOVALUTAZIONE

Q791. Il protocollo HTTPS è la combinazione di:
A. TLS e SSl
B. TLS(SSL) e FTP
C. TLS(SSL) e HTTP ma solo per casi specifici
D. TLS(SSL) e HTTP

Answer: D
Section: AUTOVALUTAZIONE

Q792. La distribuzione delle chiavi pubbliche non avviene:
A. Mediante certificati

B. Mediante la crittografia simmetrica
C. Mediante un'autorità di distribuzione
D. Attraverso l'inserimento in un elenco pubblico

Answer: B
Section: AUTOVALUTAZIONE

Q793. Nella distribuzione semplice della chiave segreta fra due utenti A e B, cosa invia l'utente B all'utente A in risposta al primo invio dell'utente A:
A. La chiave segreta di sessione da lui (utente B) generata
B. La chiave segreta di sessione da lui (utente B) generata, cifrata con la sua chiave privata
C. La chiave segreta di sessione da lui (utente B) generata, cifrata con la chiave pubblica dell'utente A
D. La chiave segreta di sessione da lui (utente B) generata, cifrata con la sua chiave pubblica

Answer: C
Section: AUTOVALUTAZIONE

Q795. Il malware Keylogger è in grado di:
A. Leggere il file system del sistema attaccato
B. Inibire l'inserimento dati da tastiera
C. Di catturare login e password di un utente sotto attacco
D. Di catturare i caratteri inseriti da tastiera

Answer: D
Section: AUTOVALUTAZIONE

Q796. La regola di firewall a filtraggio di pacchetti con Direzione=Out, Protocollo=TCP, Porta Dest= >1023 consente:
A. Traffico dati in uscita per il protocollo TCP su una porta di uscita superiore a 1023
B. Traffico dati in entrata per il protocollo TCP su una porta di ingresso superiore a 1023
C. Traffico dati in uscita per il protocollo TCP su indirizzi IP superiore a 1023
D. Traffico dati in uscita per il protocollo TCP uguale a un Kbyte

Answer: A
Section: AUTOVALUTAZIONE

Q796. La suite di protocolli ISO/OSI è:
A. Il Modello della pila di protocolli di rete definita da 7 protocolli nello standard del 1984
B. Il Modello della pila di protocolli implementati in Internet definita da 4 livelli nello standard RFC 1122 del 1989
C. Il Modello della pila di protocolli implementati in Internet definita da 4 protocolli nello standard RFC 1122 del 1989
D. Il Modello della pila di protocolli di rete definita da 7 livelli nello standard del 1984

Answer: D
Section: AUTOVALUTAZIONE

Q797. Il Multimedia Forensics analizza:
A. Hard disk
B. Contenuti multimediali
C. Smartphone
D. Chiavi USB e tablet

Answer: B
Section: AUTOVALUTAZIONE

Q799. Si definisce botnet:
A. Un Software che diffonde in rete copie dei file memorizzati su un computer infettato
B. Un attacco informatico che si ripete ad intervalli di tempo regolari su uno stesso computer
C. La rete di computer infettati che l autore di un attacco controlla
D. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server

Answer: C
Section: AUTOVALUTAZIONE

Q802. Il servizio di Integrità dei dati garantisce che:
A. Il destinatario sia autenticato
B. I dati ricevuti non sono stati modificati
C. Il mittente sia autenticato
D. La comunicazione sia cifrata

Answer: B
Section: AUTOVALUTAZIONE

Q803. Il Controllo dell'Instradamento è:
A. Un Meccanismo di Sicurezza pervasivo
B. Un Meccanismo di Sicurezza orientato alla riduzione dei tempi di trasmissione
C. Un Meccanismo di Sicurezza da utilizzare nel caso si sospetti di essere sottoposti ad attacco in certi punti della rete
D. Un Meccanismo di Sicurezza specifico orientato all'integrità dei dati

Answer: C
Section: AUTOVALUTAZIONE

Q803. In una rete di accesso a Internet FTTH il dispositivo ONT (Optical Network Terminator) effettua:
A. La conversione tra segnali ottici e segnali elettrici digitali nella centrale locale della compania telefonica e consente il collegamento ad Internet tramite un router del provider
B. Il collegamento finale tra il sistema periferico e l'edge router
C. La conversione tra segnali ottici e segnali elettrici digitali nell'abitazione dell'utente
D. Il collegamento finale tra il sistema periferico e il server del provider che gestisce la connessione

Answer: C
Section: AUTOVALUTAZIONE

Q804. Il firewall si frappone tra:
A. Due host
B. La rete interna e Internet
C. Un host e la rete interna
D. Ogni macchina in comunicazione

Answer: B
Section: AUTOVALUTAZIONE

Q807. Quali di queste affermazioni è vera per l'algoritmo HMAC:

A. Non è utilizzato per la sicurezza IP
B. La sicurezza di HMAC dipende direttamente dalla sicurezza della funzione di hash
C. La sicurezza di HMAC non dipende direttamente dalla sicurezza della funzione di hash
D. La struttura di HMAC degrada le performance delle funzioni hash utilizzate

Answer: B
Section: AUTOVALUTAZIONE

Q808. In RSA, qual è il legame tra Õ(n) e il valore e:
A. MCD(Õ(n),e)=1
B. Nessun legame
C. Õ(n)*e=1
D. Õ(n)<e

Answer: A
Section: AUTOVALUTAZIONE

Q809. In MM Forensics, nel caso della tecnica JPEG Ghost, si procede calcolando successive differenze fra:
A. L'immagine da analizzare e le sue versioni filtrate a con differenti finestre di filtro
B. L'immagine da analizzare e la sua versione compressa due volte
C. L'immagine da analizzare e le sue versioni ricompresse a differenti fattori di qualità
D. Le varie versioni dell'immagine da analizzare ricompresse a differenti fattori di qualità

Answer: C
Section: AUTOVALUTAZIONE

Q811. Una minaccia è:
A. Un potenziale pericolo
B. Un attacco
C. Un tipo di attacco
D. Una violazione

Answer: A
Section: AUTOVALUTAZIONE

Q812. Cosa si intende per crittografia simmetrica:
A. Cifratura e decifratura funzionano allo stesso modo
B. Il testo cifrato si presenta simmetrico
C. Cifratura e decifratura usano la stessa chiave
D. Cifratura e decifratura usano due chiavi tra di loro simmetriche

Answer: C
Section: AUTOVALUTAZIONE

Q814. La cifratura a blocchi è:
A. Più vantaggiosa di quella a flussi
B. Più complessa di quella a flussi
C. Basata sull'elaborazione di un blocco di testo in chiaro
D. Dipendente solo da sottoparti della chiave

Answer: C

Section: AUTOVALUTAZIONE

Q815. Le tecniche di MM Forensics stabiliscono se un'immagine è reale o è un fake ricorrendo all'uso di:
A. Analisi del contrasto dell'immagine
B. Analisi di elementi fisici o di descrittori relativi all'immagine
C. Analisi dei colori relativi all'immagine
D. Solo analizzando le caratteristiche del formato JPEG

Answer: B
Section: AUTOVALUTAZIONE

Q815. Nel protocollo TLS, la funzione pseudo-random prende in ingresso:
A. Una chiave
B. Un valore segreto e un valore seed
C. Due valori segreti e un valore seed
D. Due chiavi, di cui una generata dall'altra

Answer: B
Section: AUTOVALUTAZIONE

Q815. La cifratura a blocchi ideale non è praticabile perché:
A. Dovrebbe avere risorse infinite per la cifratura
B. Lo spazio delle chiavi possibili sarebbe limitato
C. Non sarebbe comunque sicura
D. La chiave sarebbe molto lunga

Answer: D
Section: AUTOVALUTAZIONE

Q816. Quando un malware si replica effettua:
A. La copia di un file infetto
B. La copia di se stesso sullo stesso computer o su altri
C. La copia di se stesso sullo stesso disco
D. Un'azione di attacco informatico

Answer: B
Section: AUTOVALUTAZIONE

Q816. L'algoritmo DES riceve in input:
A. Blocco dati di 64 bit e chiave di 128 bit
B. Blocco dati di 56 bit e chiave di 56 bit
C. Blocco dati di 64 bit e chiave di 56 bit
D. Blocco dati di 56 bit e chiave di 128 bit

Answer: C
Section: AUTOVALUTAZIONE

Q817. La Blockchain è:
A. Una tecnologia esclusiva per il trasferimento di denaro
B. Una tecnologia basata su Bitcoin
C. Una tecnologia che utilizza strumenti crittografici e DLT

D. Una tecnologia basata su criptovalute

Answer: C
Section: AUTOVALUTAZIONE

Q817. Il malware Rootkit permette:
A. Di accedere con profilo root su un certo sistema
B. Di mantenere coperto un accesso illecito con profilo root su un certo sistema
C. Di distribuire illecitamente i privilegi di root di un sistema
D. Di bloccare l'accesso root ad un sitema

Answer: B
Section: AUTOVALUTAZIONE

Q818. Esistono tecniche di MM Forensics che consentono di determinare se un'immagine:
A. Proviene da un social network ma non risalire alle condivisioni
B. Proviene da un social network ed eventualmente risalire alle condivisioni
C. Proviene da un social network ma se non è stata ricompressa JPEG
D. Proviene da un social network ma se non è stata modificata dal social network

Answer: B
Section: AUTOVALUTAZIONE

Q818. Un virus informatico è:
A. Un Software che diffonde in rete copie dei file memorizzati su un computer infettato
B. Un malware autoreplicante che può infettare un dispositivo senza alcuna interazione esplicita con l utente
C. La rete di computer infettati che l autore di un attacco controlla
D. Un malware autoreplicante che richiede una qualche forma di interazione con l utente per poter infettare il dispositivo

Answer: D
Section: AUTOVALUTAZIONE

Q819. Alcune tecniche di MM Forensics, per la rilevazione di immagini fake, basate sull'analisi degli elementi fisici presenti nell'immagine stessa, considerano:
A. L'inconsistenza della direzione di luce
B. L'inconsistenza della luminosità
C. L'inconsistenza del livello di grigio delle ombre
D. L'inconsistenza della forma delle ombre

Answer: A
Section: AUTOVALUTAZIONE

Q821. Nell'accesso ai "servizi nascosti" della rete Tor, dove l'utente comunica il Tor relay di rendezvous:
A. Su più Tor relay
B. Su un qualsiasi Tor relay
C. Sul Tor relay di rendezvous
D. In uno dei punti di introduzione

Answer: D
Section: AUTOVALUTAZIONE

Q821. Considerando solo il ritardo di trasmissione nella rete in figura, quando attraverso il collegamento comune di velocità R nel nucleo della rete, condiviso ad intervalli di tempo uguali, avvengono 10 trasmissioni di dati contemporane tra 10 coppie client-server , se la velocità del collegamento comune disponibile per ogni trasferimento dati diventa minore delle velocità di accesso al nucleo della rete Rc dei client e Rs dei server, il throughput medio end-to-end di una trasmissione di dati tra una coppia client-server è approssimato da:

A. Throughput medio end-to-end = (Rs+Rc)/2 bps
B. Throughput medio end-to-end = minimo(Rs, Rc) bps
C. Throughput medio end-to-end = velocità ridotta offerta dal collegamento comune
D. Throughput medio end-to-end = massimo(Rs, Rc) bps

Answer: C
Section: AUTOVALUTAZIONE

Q822. La tecnica One-Time Pad è inviolabile in quanto:

A. Non prevede l'uso di chiavi
B. La chiave è usata una sola volta
C. La chiave è molto lunga
D. La chiave è lunga quanto il testo cifrato e usata una sola volta

Answer: D
Section: AUTOVALUTAZIONE

Q823. In Kerberos V4, il TicketV per il server contiene:

A. La chiave di dialogo tra client e server
B. Nessuna chiave
C. L'AutenticatoreC del client
D. La chiave pubblica del client

Answer: A
Section: AUTOVALUTAZIONE

Q824. Nella decifratura di Feistel quale delle seguenti proprietà permette la generazione del corretto input della fase (i-1)-esima:

A. F(REi-1, Ki) •" F(REi-1, Ki)=0
B. F(REi-1, Ki) •" F(REi-1, Ki)=REi-1
C. F(REi-1, Ki) •" F(REi-1, Ki)=Ki
D. F(REi-1, Ki) •" F(REi-1, Ki)=1

Answer: A
Section: AUTOVALUTAZIONE

Q825. L'algoritmo AES risolve il difetto di 3DES di:

A. Lunghezza chiave ridotta
B. Implementazione software molto lenta
C. Cifratura diversa dalla decifratura
D. Non sicurezza rispetto ad attacchi a forza bruta

Answer: B
Section: AUTOVALUTAZIONE

Q825. In una rete di accesso a Internet DSL lo splitter che si trova nell'abitazione dell'utente effettua:
A. Il collegamento diretto tra il sistema periferico e l'edge router
B. La conversione del segnale analogico proveniente dalla rete telefonica nel formato digitale e lo invia ai sistemi periferici
C. La suddivisione del segnale proveniente dalla linea telefonica esterna all'abitazione, separando il segnale analogico del traffico vocale dal segnale analogico del traffico dati, e invia questi segnali all apparecchio telefonico ed al modem mediante collegamenti separati
D. Il collegamento diretto tra il sistema periferico e il server del provider che gestisce la connessione

Answer: C
Section: AUTOVALUTAZIONE

Q826. Il firewall a filtraggio di pacchetti IP può operare:
A. A livello di applicazione
B. A livello fisico
C. A livello di indirizzi sorgente/destinazione
D. Ad ogni livello

Answer: C
Section: AUTOVALUTAZIONE

Q826. In una rete a commutazione di pacchetto il ritardo di nodo è:
A. Il tempo impiegato dal nodo per determinare il canale di trasmissione in uscita in base all'indirizzo di destinazione del pacchetto
B. Il ritardo dell'attesa in coda di un pacchetto memorizzato nel buffer di output quando il canale di trasmissione in uscita è occupato
C. Il ritardo per la determinazione della tabella di inoltro nella trasmissione store and forward relativa al collegamento in uscita dal nodo
D. La somma dei ritardi di elaborazione, accodamento, trasmissione e propagazione relativi al collegamento in uscita dal nodo

Answer: D
Section: AUTOVALUTAZIONE

Q827. Il CFA serve a:
A. Ad unire le tre componenti di colore
B. A interploare le tre componenti di colore
C. Far passare le tre componenti di colore
D. Filtrare le componenti di colore

Answer: D
Section: AUTOVALUTAZIONE

Q830. In Blockchain, un attaccante che sia riuscito a ricalcolare una blockchain "modificata" è in grado di:
A. Alterare il Ledger distribuito inviando a tutti la nuova blockchain
B. Alterare il Ledger distribuito
C. Alterare il Ledger distribuito solo se guadagna il consenso della metà più uno dei nodi della rete P2P
D. Alterare il Ledger distribuito solo se guadagna il consenso di alcuni nodi della rete P2P

Answer: C
Section: AUTOVALUTAZIONE

Q830. Quale di queste definizioni meglio definisce X.509:
A. Definisce la tipologia di crittografia pubblica da usare con i certificati
B. Definisce il formato dei certificati
C. Rappresenta un framework per servizi di autenticazione basato sull'uso di un repository e di certificati
D. Rappresenta un framework per servizi di crittografia pubblica basato sull'uso di un repository e di certificati

Answer: C
Section: AUTOVALUTAZIONE

Q834. Un attacco alla sicurezza è:
A. Qualsiasi azione che compromette la sicurezza delle informazioni
B. Processo progettato per rilevare, prevenire o riparare i danni prodotti da un attacco alla sicurezza
C. Servizio che migliora la sicurezza dei sistemi di elaborazione e trasmissione
D. La cancellazione di informazioni

Answer: A
Section: AUTOVALUTAZIONE

Q834. Nel modello generale per la sicurezza di rete esistono sempre:
A. Una terza parte fidata
B. Un componente per la trasformazione delle informazioni
C. Un attaccante che intercetta il messaggio
D. Un componente per l'accesso alle informazioni segrete

Answer: B
Section: AUTOVALUTAZIONE

Q835. Quale delle seguenti non è una differenza fra SSL e TLS:
A. Usano diversi codici MAC
B. TLS usa una funzione di espansione dei valori segreti
C. TLS supporta codici di allarme addizionali
D. SSL si appoggia sul livello TCP mentre TLS sul livello IP

Answer: D
Section: AUTOVALUTAZIONE

Q843. La crittografia asimmetrica che usa in cifratura la chiave pubblica del destinatario può garantire:
A. Autenticazione e segretezza
B. Segretezza ma non autenticazione
C. Autenticazione ma non segretezza
D. Né autenticazione né segretezza

Answer: B
Section: AUTOVALUTAZIONE

Q844. Una volta che un "miner" ha trovato la soluzione deve:
A. Aggiungere il nuovo blocco alla blockchain
B. Richiedere la ricompensa in BTC
C. Pubblicarla agli altri nodi
D. Pubblicarla nel Ledger

Answer: C
Section: AUTOVALUTAZIONE

Q846. Nel protocollo Mix, il messaggio del mittente verso il destinatario è cifrato nel seguente ordine:
A. Non esiste un ordine definito
B. Prima la cifratura relativa all'ultimo proxy e poi le altre
C. Prima la cifratura relativa al primo proxy e poi le altre
D. Prima la cifratura relativa all'ultimo proxy e poi quella relativa al primo proxy

Answer: B
Section: AUTOVALUTAZIONE

Q846. Il protocollo SSL è costituito da dei sotto-protocolli con le seguenti caratteristiche:
A. Due protocolli allo stesso livello
B. Un protocollo di base e tre protocolli a livello superirore
C. Due protocolli a differenti livelli
D. Un protocollo di base e uno a livello superiore

Answer: B
Section: AUTOVALUTAZIONE

Q847. Nell'infrastruttura PKIX per X.509, quale delle seguenti entità può non essere presente:
A. L'autorità di certificazione
B. L'utente finale
C. Il repository dei certificati
D. L'emettitore della CRL

Answer: D
Section: AUTOVALUTAZIONE

Q848. In IPSec, esiste la necessità di impiegare combinazioni di SA per:
A. Non esiste una necessità
B. Implementare servizi di sicurezza diversi
C. Modificare i servizi di sicurezza in essere
D. Implementare più volte lo stesso servizio di sicurezza

Answer: B
Section: AUTOVALUTAZIONE

Q849. Nella distribuzione delle chiavi pubbliche, quale vantaggio dà usare i certificati rispetto al caso di adottare un'autorità di distribuzione:
A. Evita interazioni continue con l'autorità di distribuzione
B. Nessun vantaggio
C. Evita di doversi scambiare le chiavi pubbliche
D. Non ci sono autorità di garanzia

Answer: A
Section: AUTOVALUTAZIONE

Q850. Uno dei principali dubbi su DES riguardava:

A. La ridotta dimensione del blocco dati
B. La ridotta dimensione della lunghezza della chiave
C. La ridotta dimensione della chiave rispetto a quello dell'algoritmo iniziale
D. La complessità computazionale

Answer: C
Section: AUTOVALUTAZIONE

Q850. Una DoS provocata da una inondazione di banda è:
A. Una interruzione del servizio causata dall'invio ad una applicazione vulnerabile o al Sistema Operativo in esecuzione sul server sotto attacco, di una sequenza di pacchetti opportunamente costruiti per determinare il blocco del servizio o anche lo spegnimento del server
B. Una interruzione del servizio causata dall'invio da parte dell'attaccante di una grande quantità di pacchetti capace di occupare completamente il collegamento di accesso del server
C. Una interruzione del servizio causata da una gran numero di connessioni TCP generate dall'attaccante e mantenute tutte aperte per ingorgare la capacità ricettiva del server
D. La diffusione in rete di copie dei file memorizzati su un computer

Answer: B
Section: AUTOVALUTAZIONE

Q851. Nello standard SET, per verificare la doppia firma il venditore e la banca eseguono una stessa operazione:
A. Nessuna operazione comune
B. L'hash delle informazioni dell'ordine
C. La decifratura della doppia firma con la chiave pubblica del cliente
D. La decifratura della doppia firma con la chiave privata del cliente

Answer: C
Section: AUTOVALUTAZIONE

Q852. Negli algoritmi hash di tipologia SHA, il numero delle fasi è dell'ordine di:
A. circa 10
B. circa 20
C. circa 100
D. circa 1000

Answer: C
Section: AUTOVALUTAZIONE

Q852. La cifratura di Feistel:
A. Usa una chiave molto lunga
B. Usa un numero elevato di fasi
C. Usa una dimensione del blocco e della chiave praticabile
D. Usa algoritmi diversi in cifratura e decifratura

Answer: C
Section: AUTOVALUTAZIONE

Q853. La Network Forensics si occupa di:
A. Monitorare e analizzare il traffico di rete fra computer
B. Impedire l'accesso a un sistema

C. Impedire la diffusione di malware in rete
D. Monitorare e analizzare il traffico di fra due computer

Answer: A
Section: AUTOVALUTAZIONE

Q853. I 56 bit della chiave DES:
A. Sono divisi in due metà ciascuna delle quali subisce delle trasformazioni indipendenti
B. Sono divisi in due metà ciascuna delle quali subisce le stesse trasformazioni
C. Sono divisi in due metà una delle quali non subisce trasformazioni
D. Sono divisi in due metà ma il risultato della permutazione ottenuta è lo stesso

Answer: A
Section: AUTOVALUTAZIONE

Q854. In una rete a commutazione di pacchetto il ritardo di accodamento relativo ad un collegamento in uscita da un router è il tempo che:
A. Il router impiega per gestire la coda dei pacchetti memorizzati nel buffer di output relativi ad una trasmissione dati tra la sorgente e la destinazione
B. Il router aspetta per completare la ricezione di tutti i bit che compongono il pacchetto che vengono memorizzati nel buffer di output
C. Un pacchetto rimane nella coda di attesa memorizzata nel buffer di output, prima di essere inviato sul collegamento di uscita del router
D. La destinazione aspetta per completare la ricezione di tutti i bit che compongono il pacchetto che vengono memorizzati nel buffer di output

Answer: C
Section: AUTOVALUTAZIONE

Q855. Le tecniche di MM Forensics non consentono di stabilire se:
A. Un'immagine è stata acquisita da una certo modello di fotocamera
B. Un'immagine è stata acquisita da una certa marca di fotocamera
C. Un'immagine è stata acquisita da un certo dispositivo di fotocamera
D. Un'immagine è stata acquisita dal proprietario di un certo dispositivo

Answer: D
Section: AUTOVALUTAZIONE

Q856. Se i certificati X.509 sono emessi da CA diverse accade che:
A. Gli utenti non possono comunicare
B. Non ci sono problemi le CA sono autenticate fra di loro
C. Gli utenti possono comunicare ma devono inviare i loro messaggi alle rispettive CA
D. Gli utenti possono comunicare ma devono inviare i loro messaggi ad una delle due CA

Answer: B
Section: AUTOVALUTAZIONE

Q856. La denominazione dei pacchetti relativi ai livelli del Modello TCP/IP è:
A. Messaggio per il livello di applicazione, datagramma per il livello di trasporto, segmento per il livello di rete, frame per il livello di collegamento, il singolo bit per il livello fisico
B. Messaggio per il livello di applicazione, segmento per il livello di trasporto, frame per il livello di rete, datagramma

per il livello di collegamento, il singolo bit per il livello fisico
C. Messaggio per il livello di applicazione, segmento per il livello di trasporto, datagramma per il livello di rete, frame per il livello di collegamento, il singolo bit per il livello fisico
D. Messaggio per il livello di applicazione, frame per il livello di trasporto, segmento per il livello di rete, datagramma per il livello di collegamento, il singolo bit per il livello fisico

Answer: C
Section: AUTOVALUTAZIONE

Q856. Il livello di Trasporto dello standard ISO/OSI offre servizi:
A. Che consentono la comunicazione tra i nodi della rete che vengono attraversati nel percorso che va dal sistema periferico sorgente al sistema periferico destinazione
B. Che permettono un trasferimento di dati affidabile, effettuando anche un controllo degli errori e delle perdite di pacchetti tra due sistemi periferici
C. Per il trasferimento di dati tra nodi adiacenti attraverso il tipo di collegamento che sussiste tra di loro
D. Necessari a livello Hardware per controllare il flusso di dati attraverso i collegamenti e le connessioni ai dispositivi che permettono il passaggio dei segnali che rappresentano le informazioni

Answer: B
Section: AUTOVALUTAZIONE

Q857. Quale delle seguenti affermazioni in merito alle comunicazioni anonime è corretta:
A. Effettuare la comunicazione con un proxy garantisce sempre l'anonimato del mittente
B. La crittografia non è sufficiente a garantire anonimato
C. Effettuare la comunicazione con un proxy garantisce sempre l'anonimato
D. La crittografia è sufficiente a garantire anonimato

Answer: B
Section: AUTOVALUTAZIONE

Q857. Per generare l'hash di un blocco della Blockchain, i dati che vengono passati in input all'hash sono:
A. L'hash del blocco precedente e il nonce
B. I dati delle transazioni del blocco attuale, l'hash del blocco precedente e il nonce
C. I dati delle transazioni del blocco attuale e l'hash del blocco precedente
D. I dati delle transazioni del blocco attuale, l'hash del blocco precedente, il nonce del blocco precedente e di quello attuale

Answer: B
Section: AUTOVALUTAZIONE

Q857. In IPSec, quale dei protocolli garantisce un set completo di servizi di sicurezza:
A. AH
B. ESP
C. ESP con l'opzione di autenticazione
D. Nessuno dei protocolli

Answer: C
Section: AUTOVALUTAZIONE

Q859. I "miner" svolgono il compito primario di:
A. Aggiungere un nuovo blocco alla blockchain

B. Risolvere un problema crittografico complesso
C. Verificare le soluzioni delle PoW
D. Aggiornarsi sulla rete P2P

Answer: B
Section: AUTOVALUTAZIONE

Q861. Quale delle seguenti affermazioni sul Deep Web è vera:
A. Nel Deep Web ci sono solo contenuti proibiti
B. Nel Deep Web ci sono pagine indicizzate
C. Nel Deep Web ci sono le pagine non indicizzate
D. Il Deep Web è solo una porzione ridotta del web

Answer: C
Section: AUTOVALUTAZIONE

Q861. Il codice MAC garantisce:
A. La segretezza
B. La firma
C. L'autenticazione
D. L'autenticazione e la segretezza

Answer: C
Section: AUTOVALUTAZIONE

Q862. In IPSec, il protocollo ESP, diversamente da AH, garantisce:
A. La modalità tunnel
B. L'accesso da remoto
C. La segretezza
D. L'autenticazione

Answer: C
Section: AUTOVALUTAZIONE

Q863. In PGP, la compressione ZIP si effettua:
A. Dopo aver applicato la crittografia simmetrica
B. Dopo aver applicato la firma ma prima della crittografia simmetrica
C. Non si applica
D. Dopo aver applicato la crittografia simmetrica ma prima della firma

Answer: B
Section: AUTOVALUTAZIONE

Q864. Nella cifratura Playfair una coppia di lettere viene:
A. Codificata in una terna di lettere
B. Codificata in una coppia di lettere dipendente dalla posizione relativa di tali lettere nella tabella di cifratura
C. Codificata in più coppie di lettere
D. Codificata in una coppia permutata

Answer: B
Section: AUTOVALUTAZIONE

Q865. Nel protocollo di distribuzione delle chiavi, cosa contiene il messaggio di risposta del KDC all'utente A
A. La chiave di sessione
B. La chiave di sessione, il messaggio inviato da A e il messaggio da inviare a B cifrato con la chiave di B
C. La chiave di sessione e il messaggio da inviare a B cifrato con la chiave di B
D. La chiave di sessione e il messaggio da inviare a B cifrato con la chiave di B

Answer: B
Section: AUTOVALUTAZIONE

Q867. Il campo payload di un pacchetto gestito al livello di Rete è costituito da:
A. Un Segmento fornito dal livello di Trasporto
B. Un Messaggio fornito dal livello di Applicazione
C. Un Datagramma fornito dal livello di Rete
D. Un Frame fornito dal livello di Collegamento

Answer: A
Section: AUTOVALUTAZIONE

Q868. In PGP, la conversione radix-64 trasforma:
A. Un gruppo di 8 bit in un carattere ASCII
B. Un gruppo di 6 bit in altri 6 bit permutati
C. Un gruppo di 16 bit in un carattere ASCII
D. Un gruppo di 6 bit in un carattere ASCII

Answer: D
Section: AUTOVALUTAZIONE

Q868. Nel caso di MAC basato su crittografia DES e CBC, il checksum di uscita è costituito da:
A. L'output della cifratura DES applicata allo XOR fra l'ultimo blocco del messaggio e la cifratura DES al penultimo passo
B. L'operazione di XOR fra l'output della cifratura DES dell'ultimo blocco del messaggio e il blocco precedente
C. L'operazione di XOR fra l'output della cifratura DES dell'ultimo blocco del messaggio e la chiave
D. L'operazione di XOR fra l'output della cifratura DES di tutti blocchi del messaggio

Answer: A
Section: AUTOVALUTAZIONE

Q869. L insieme delle misure adottate per proteggere i dati durante la loro trasmissione attraverso una serie di reti interconnesse:
A. Computer Security
B. Network Security
C. Internet Security
D. Access Security

Answer: C
Section: AUTOVALUTAZIONE

Q870. In Blockchain, ognuno dei nodi della rete P2P possiede:
A. Una versione del Ledger non pubblica
B. Una versione del Ledger
C. Una versione del Ledger sincronizzata

D. Una versione del Ledger e l'ultimo blocco

Answer: C
Section: AUTOVALUTAZIONE

Q871. Il firewall monitora il traffico dati:
A. In ingresso
B. In uscita
C. In ingresso e in uscita
D. In ingresso e in uscita solo da alcuni host

Answer: C
Section: AUTOVALUTAZIONE

Q871. In IPSec, con il protocollo ESP si può realizzare:
A. Il servizio di autenticazione e opzionalmente il servizio di segretezza
B. Il servizio di segretezza e opzionalmente il servizio di autenticazione
C. Solo il servizio di segretezza
D. Il servizio di autenticazione

Answer: B
Section: AUTOVALUTAZIONE

Q874. In SSL, il protocollo Handshake serve a:
A. Autenticazione del client
B. Autenticazione vicendevole del server e del client
C. Autenticazione del server
D. Inviare il codice MAC

Answer: B
Section: AUTOVALUTAZIONE

Q874. L'algoritmo HMAC è:
A. Un algoritmo MAC basato su una funzione hash
B. Un algoritmo hash basato su una funzione di crittografia
C. Un algoritmo MAC basato su una funzione di crittografia
D. Un algoritmo MAC non basato su una funzione hash

Answer: A
Section: AUTOVALUTAZIONE

Q875. Nella trasmissione in Internet un pacchetto è costituito da:
A. Un bit del messaggio trasmesso ed informazioni aggiuntive che identificano la destinazione del messaggio
B. Una parte della sequenza del messaggio trasmesso
C. Tutto il messaggio trasmesso suddiviso in parti
D. Una parte della sequenza del messaggio trasmesso ed informazioni aggiuntive che identificano la destinazione del messaggio

Answer: D
Section: AUTOVALUTAZIONE

Q878. L'algoritmo AES usa:
A. Una dimensione di blocco di 64 bit
B. Una dimensione di blocco di 128 bit e chiave di 56 bit
C. Una dimensione di blocco di 128 bit e chiave di 128 bit
D. Una dimensione di blocco di 128 bit e chiave di qualsiasi lunghezza

Answer: C
Section: AUTOVALUTAZIONE

Q879. Quali di questi processi o sistemi lascia una traccia sull'immagine durante la fase di acquisizione:
A. Il sensore ma non il sistema ottico
B. Il sensore e il processing interno alla fotocamera
C. Il sensore ma solo a certe risoluzioni
D. Il sensore ma dipende dal tipo di immagine

Answer: B
Section: AUTOVALUTAZIONE

Q879. In una trasmissione store and forward il tempo di trasmissione di un solo pacchetto di L bit da una sorgente ad una destinazione entrambe connesse ad un router da collegamenti con velocità di trasmissione R bps è:
A. L/R secondi
B. 2L/R secondi
C. 2L-R secondi
D. L-R secondi

Answer: B
Section: AUTOVALUTAZIONE

Q881. La strutturazione di Internet come reti di reti consiste:
A. Nella suddivisione delle reti degli ISP in gruppi corrispondenti a tre livelli di una gerachia dove: gli ISP di accesso che hanno come clienti gli utenti finali costituiscono il livello più basso e pagano il proprio traffico dati agli ISP regionali posti nel livello superiore, che a loro volta sono clienti degli ISP di livello 1, posti nel grado più alto della gerarchia che non pagano per il proprio traffico dati. A questa gerarchia si aggiungono le reti private dei distributori di contenuti, di cui Google è un esempio
B. Nella suddivisione delle reti degli ISP in gruppi corrispondenti a due livelli di una gerachia dove: gli ISP di accesso che hanno come clienti gli utenti finali costituiscono il livello più basso e pagano il proprio traffico dati agli ISP regionali posti nel livello superiore che pagano in funzione del traffico dati che si scambiano tra loro. A questa gerarchia si aggiungono le reti private dei distributori di contenuti, di cui Google è un esempio
C. Nella suddivisione delle reti in due gruppi costituiti dalle reti pubbliche degli ISP di accesso che forniscono traffico agli utenti finali mediante tecnologie di trasmissione di vario tipo (DDL, FTTH, Wi-Fi, satellitare) e dalle reti private che si occupano di distribuire contenuti, di cui Google è un esempio
D. Nella rete costituita dalla connessione tra le sottoreti degli ISP di accesso che forniscono traffico agli utenti finali mediante tecnologie di trasmissione di vario tipo (DDL, FTTH, Wi-Fi, satellitare). A questa rete di reti si aggiungono le reti private dei distributori di contenuti, di cui Google è un esempio

Answer: A
Section: AUTOVALUTAZIONE

Q882. Nello scambio di chiavi Diffie-Hellman, con un attacco a forza bruta l'attaccante dovrebbe calcolare Ya = a (Xa) mod q conoscendo:
A. Ya

B. Ya, il valore a e il valore q
C. Ya e il valore q
D. Ya, Xa e il valore q

Answer: B
Section: AUTOVALUTAZIONE

Q883. Per garantire segretezza, autenticazione e firma, in cifratura asimmetrica si devono usare:
A. La chiave privata del mittente e poi la chiave pubblica del destinatario
B. La chiave privata del destinatario e poi la chiave pubblica del mittente
C. La chiave pubblica del destinatario e poi la chiave pubblica del mittente
D. La chiave pubblica del destinatario e poi la chiave privata del mittente

Answer: A
Section: AUTOVALUTAZIONE

Q884. Il codice MAC per garantire la segretezza ha bisogno di:
A. Cifratura a chiave pubblica
B. Due chiavi distinte
C. Due chiavi uguali
D. Non può garantire segretezza

Answer: B
Section: AUTOVALUTAZIONE

Q885. La sicurezza dell'algoritmo RSA sta:
A. Nell'uso di una chiave pubblica
B. Nella segretezza delle due chiavi
C. Nella difficoltà dell'operazione di fattorizzazione di grandi numeri
D. Nella difficoltà dell'operazione di fattorizzazione

Answer: C
Section: AUTOVALUTAZIONE

Q888. Nell'accesso ai "servizi nascosti" della rete Tor, cosa rappresenta un relay di rendezvous:
A. Un Tor relay selezionato dall'utente per ricevere il servizio
B. Un Tor relay di guardia
C. Un relay scelto fra i punti di introduzione
D. Un Tor relay selezionato dal "servizio nascosto" per erogarvi il servizio

Answer: A
Section: AUTOVALUTAZIONE

Q888. Con il termine Cavallo di Troia si indica un malware:
A. All'interno di un altro programma apparentemente innocuo
B. All'interno di un altro malware
C. Una serie di malware
D. Una rete di malware

Answer: A
Section: AUTOVALUTAZIONE

Q889. Cosa si intende col termine criptologia:
A. L''insieme di crittografia e analisi crittografica
B. La cripto-analisi
C. L'insieme delle tecniche di attacco crittografico
D. L'insieme di tecniche per la crittografia

Answer: A
Section: AUTOVALUTAZIONE

Q889. In una rete di calcolatori, il throughput medio end-to-end di una trasmissione di dati tra due sistemi periferici è dato da:
A. Throughput medio end-to-end = T/F bps, dove F è il numero di bit trasmessi tra i due sistemi periferici e T il tempo richiesto dalla trasmissione di tutti i bit
B. Throughput medio end-to-end = F/T bps, dove F è il numero di bit trasmessi tra i due sistemi periferici e T il tempo richiesto dalla trasmissione di tutti i bit
C. Throughput medio end-to-end = 2F/T bps, dove F è il numero di bit trasmessi tra i due sistemi periferici e T il tempo richiesto dalla trasmissione di tutti i bit
D. Throughput medio end-to-end = F+T bps, dove F è il numero di bit trasmessi tra i due sistemi periferici e T il tempo richiesto dalla trasmissione di tutti i bit

Answer: B
Section: AUTOVALUTAZIONE

Q890. Il Multimedia Forensics è un settore specifico del:
A. Forensics
B. Digital Forensics
C. Computer Forensics
D. Image Forensics

Answer: B
Section: AUTOVALUTAZIONE

Q890. La crittografia di canale:
A. Viene eseguita tra ogni collegamento vulnerabile
B. Viene eseguita solo tra alcuni nodi principali di collegamento
C. Viene eseguita solo tra i nodi terminali della trasmissione
D. Viene eseguita a livello alti della gerarchia OSI

Answer: A
Section: AUTOVALUTAZIONE

Q891. I vantaggi base offerti da Blockchain sono:
A. Trasferimenti di denaro più veloci ma con costi superiori
B. Transazioni quasi istantanee, senza intermediari e costi ridotti
C. Trasferimenti di denaro quasi istantanei e costi ridotti verso la banca
D. Zero commissioni bancarie

Answer: B
Section: AUTOVALUTAZIONE

Q897. Quale delle seguenti espressioni non rappresenta una funzione hash:
A. H(x)=h
B. G(k)=m
C. G(k,M)=h
D. G(h)=k

Answer: C
Section: AUTOVALUTAZIONE

Q898. Nel protocollo Mix, si implementa anche un'operazione di "mixing" che consiste nel:
A. Raccogliere richieste in un certo intervallo di tempo e mescolarle
B. Inviare traffico "dummy"
C. Raccogliere richieste in un certo intervallo di tempo e reinoltrarle con ritardi definiti
D. Raccogliere richieste in un certo intervallo di tempo e reinoltrarle in ordine casuale

Answer: D
Section: AUTOVALUTAZIONE

Q899. Qual è il concetto che sta dietro la necessità di comunicazioni anonime:
A. Svolgere attività fraudolente
B. Proteggere i messaggi dei soggetti coinvolti
C. Proteggere le identità dei soggetti coinvolti
D. Accedere ad informazioni compromettenti

Answer: C
Section: AUTOVALUTAZIONE

Q902. Nell'Attacco MitM si confrontano:
A. Tutti i possibili testi cifrati con K2 a partire da P con i corrispettivi testi decifrati con K1 a partire da C
B. Tutti i possibili testi cifrati con K1 a partire da P con i corrispettivi testi decifrati con K1 a partire da C
C. Tutti i possibili testi cifrati con K1 a partire da P con i corrispettivi testi decifrati con K2 a partire da C
D. Solo due testi cifrati con K2 e K1 a partire da P

Answer: C
Section: AUTOVALUTAZIONE

Q904. Se un attaccante modifica un dato di un blocco della Blockchain succede che:
A. Tutti i blocchi della Blockchain sono invalidati
B. Il blocco attuale e tutti quelli successivi della Blockchain sono invalidati
C. Cambiano solo gli hash del blocco attuale e del successivo
D. Cambiano i nonce del blocco attuale e del successivo

Answer: B
Section: AUTOVALUTAZIONE

Q905. Le tecniche di MM Forensics permettono di stabilire se un contenuto multimediale sia o meno un falso basandosi su:
A. I metadati associati ad un file multimediale
B. L'analisi visiva di un'immagine o di un video
C. L analisi di caratteristiche intrinseche di un contenuto multimediale
D. Il tipo di formato

Answer: C
Section: AUTOVALUTAZIONE

Q906. Nel protocollo HTTPS non vengono cifrati:
A. L'URL della risorsa richiesta
B. I contenuti della risorsa
C. I contenuti dell'header HTTP
D. L'intestazione IP

Answer: D
Section: AUTOVALUTAZIONE

Q908. Se un "miner" che sta risolvendo una PoW viene battuto sul tempo da un altro deve:
A. Finire di risolvere la PoW
B. Controllare la soluzione trovata dall'altro
C. Riuscire a trovare la soluzione anche se in breve tempo
D. Disconnettrsi dalla rete P2P

Answer: B
Section: AUTOVALUTAZIONE

Q908. Nello standard SET, la fase di cattura del pagamento avviene tra:
A. Il venditore e il cliente
B. Il venditore e l'emettitore
C. Il venditore e il gateway di pagamento
D. Il cliente e il gateway di pagamento

Answer: C
Section: AUTOVALUTAZIONE

Q910. Il principio che sta alla base del MMForensics è:
A. Tutti i documenti multimediali portano con sé delle tracce
B. La creazione di un contenuto multimediale contiene una traccia
C. Ogni elaborazione effettuata su un documento multimediale ne altera i metadati
D. Ogni elaborazione effettuata su un documento multimediale lascia una traccia

Answer: D
Section: AUTOVALUTAZIONE

Q910. Nel protocollo TLS è prevista un'operazione di padding del tipo:
A. Tale da ottenere una lunghezza totale multipla della dimensione dell'intestazione
B. Tale da ottenere una lunghezza totale multipla della dimensione del blocco
C. Tale da ottenere un numero di blocchi multiplo di 128
D. Tale da ottenere la lunghezza totale minima di multipli della dimensione del blocco

Answer: B
Section: AUTOVALUTAZIONE

Q910. In SSL, il protocollo SSL Record fornisce due servizi:
A. Un servizio di integrità e un servizio di segretezza

B. Un servizio di integrità e un servizio di hash
C. Un servizio di cifratura simmetrica e uno di cifratura asimmetrica
D. Un servizio di firma digitale e di anonimato

Answer: A
Section: AUTOVALUTAZIONE

Q913. In PGP, si realizza autenticazione e segretezza tramite:
A. La chiave privata del mittente, la chiave segreta di sessione e la chiave pubblica del destinatario
B. La chiave privata del mittente e la chiave pubblica del destinatario
C. La chiave privata del mittente e la chiave segreta di sessione
D. Non è realizzabile

Answer: A
Section: AUTOVALUTAZIONE

Estrazione del 04/06/2023

Se c'è un errore o un disallineamento segnalalo!

Questo documento è frutto di ore di lavoro, ma libero.

NON SBORSARE SOLDI PER AVERLO.

NO DOCSITY e DERIVATI

CERCAMI SU TELEGRAM CON L31