

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

- ☐ a. `openssl pkeyutl -encrypt -inkey pub.pem -in plain.txt -pubout -out cipher.txt`
- ☐ b. `openssl pkeyutl -encrypt -inkey pub.pem -in plain.txt -out cipher.txt`
- ☒ c. `openssl pkeyutl -encrypt -pubin -inkey pub.pem -in plain.txt -out cipher.txt` ✓
- ☐ d. Nessuna delle altre tre scelte.

Risposta corretta.

La risposta corretta è:

`openssl pkeyutl -encrypt -pubin -inkey pub.pem -in plain.txt -out cipher.txt`

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

La risposta corretta è:

L'analisi dinamica black box rappresenta un approccio superficiale per la comprensione di un malware.

da 10

a errata

gio

o 0 su 2

ssegna

da

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

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

- ☐ a. $p = 7$ e $g = 2$.
- ☒ b. $p = 5$ e $g = 1$.
- ☐ c. $p = 4$ e $g = 3$.
- ☐ d. $p = 5$ e $g = 2$.

✗

Risposta errata.

La risposta corretta è:

$p = 5$ e $g = 2$.

nda 11

sta errata

ggio

uto 0 su 2

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

- ☐ a. `openssl enc -aes-256-cbc -in FileInChiaro -out`

Domanda 8

Risposta
corretta

Punteggio
ottenuto 1 su 1



Contrassegna
domanda

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

- ☐ a. `openssl pkey -in keyA.pem -out pubA.pem`
- ☒ b. `openssl pkey -in keyA.pem -pubout -out pubA.pem` ✓
- ☐ c. Nessuna delle altre tre scelte.
- ☐ d. `openssl pkeyutl -in keyA.pem -out pubA.pem`

Risposta corretta.

La risposta corretta è:

`openssl pkey -in keyA.pem -pubout -out pubA.pem`

Domanda 9

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

- ☐ a. L'analisi dinamica black box rappresenta un approccio superficiale per la comprensione di un malware.
- ☐ b. L'analisi dinamica white box non può portare all'infezione del sistema su cui essa viene effettuata.
- ☐ c. Nessuna delle altre tre scelte.

MacBook Pro

domanda 3

risposta errata

punteggio

ottenuto 0 su 2

contrassegna

domanda

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

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

- ☒ a. $C_i = M_i \text{ XOR } E_{\{k \text{ XOR } i\}}(C_{\{i-1\}})$, con $C_0 = IV$ ✗
- ☐ b. $C_i = M_i \text{ XOR } E_k(C_{\{i-1\}})$, con $C_0 = IV$
- ☐ c. $C_i = C_{\{i-1\}} \text{ XOR } E_k(M_i)$, con $C_0 = IV$
- ☐ d. $C_i = M_i \text{ XOR } E_k(M_i \text{ XOR } C_{\{i-1\}})$, con $C_0 = IV$

Risposta errata.

La risposta corretta è:

$$C_i = M_i \text{ XOR } E_k(C_{\{i-1\}}), \text{ con } C_0 = IV$$

domanda 4

risposta errata

punteggio

ottenuto 0 su 2

contrassegna

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

Alla luce delle conoscenze attuali:

- ☐ a. Non si sa se rompere AES 256 e rompere RSA

Domanda 2

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

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

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

☐ a. $e=5$.

☒ b. $e=9$.

☐ c. $e=3$.

☐ d. $e=4$.



Risposta errata.

La risposta corretta è:
 $e=5$.

Domanda 3

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

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

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

☒ a. $C_i = M_i \text{ XOR } E_{\{k \text{ XOR } i\}}(C_{i-1})$, con

$C_0 = IV$



MacBook Pro

Risposta errata.

La risposta corretta è:

Nessuna delle altre tre scelte.

Domanda 19


Risposta
corretta

Punteggio
ottenuto 1 su 1



Contrassegna
domanda

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

- ☐ a. openssl genrsa -out rsaprivatekey.pem -passout pass:P1pp0B4ud0 -aes128 1024 -F4
- ☐ b. openssl genrsa -out rsaprivatekey.pem -passout pass:P1pp0B4ud0 -aes128 1024
- ☐ c. openssl genrsa -out rsaprivatekey.pem -aes128 1024
- ☒ d. Nessuna delle altre tre scelte. 

Risposta corretta.

La risposta corretta è:

Nessuna delle altre tre scelte.

Domanda 20


Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna

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

- ☒ a. Nessuna delle altre tre scelte. 
- ☐ b. Utilizzando Base64 per codificare la stringa

MacBook Pro

algoritmo efficiente per rompere uno dei due può essere usato per rompere l'altro.

Domanda 5

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

- ☐ a. Nessuna delle altre tre scelte.
- ☐ b. `openssl sha256 -sign -pubin priv.pem -out firma.txt plain.txt`
- ☐ c. `openssl sha256 -sign priv.pem -out firma.txt plain.txt`
- ☒ d. `openssl dgst -sha256 -sign priv.pem -out firma.txt plain.txt` ✗

Risposta errata.

La risposta corretta è:

`openssl sha256 -sign -pubin priv.pem -out firma.txt plain.txt`

Domanda 6

Risposta errata

Punteggio
ottenuto 0 su 2

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

Alla luce delle conoscenze attuali:

Domanda 18

Risposta errata

Punteggio
ottenuto 0 su 1Contrassegna
domanda

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

- ☐ a. È possibile effettuare il "resume" di una sessione in base al valore del campo *client_version*.
- ☐ b. Nessuna delle altre tre scelte.
- ☒ c. È possibile effettuare il "resume" di una sessione anche se Client e Server non hanno memorizzato i parametri di sessione. ✗
- ☐ d. È possibile effettuare il "resume" di una sessione mediante il *Change Cipher Spec* Protocol.

Risposta errata.

La risposta corretta è:

Nessuna delle altre tre scelte.

Domanda 19

Risposta
correttaPunteggio
ottenuto 1 su 1Contrassegna
domanda

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

- ☐ a. `openssl genrsa -out rsaprivatekey.pem -passout pass:P1pp0B4ud0 -aes128 1024 -F4`
- ☐ b. `openssl genrsa -out rsaprivatekey.pem -`

Domanda 6

Risposta errata

Punteggio
ottenuto 0 su 2Contrassegna
domanda

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

Alla luce delle conoscenze attuali:

- ☒ a. Fattorizzare n e rompere RSA sono due problemi non correlati tra loro. ✗
- ☐ b. Se si trovasse un algoritmo efficiente per rompere RSA allora lo si potrebbe usare per fattorizzare efficientemente n .
- ☐ c. Se si trovasse un algoritmo efficiente per fattorizzare n allora lo si potrebbe usare per rompere RSA.
- ☐ d. Fattorizzare n è equivalente computazionalmente a rompere RSA.

Risposta errata.

La risposta corretta è:

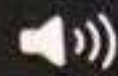
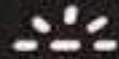
Se si trovasse un algoritmo efficiente per fattorizzare n allora lo si potrebbe usare per rompere RSA.

Domanda 7

Risposta errata

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

MacBook Pro



La risposta corretta è:

$$L_{\{i+1\}} = R_i \text{ e } R_{\{i+1\}} = L_i \text{ XOR } f(R_i, K_{\{i+1\}})$$

Domanda 14

Risposta
corretta

Punteggio
ottenuto 2 su 2



Contrassegna
domanda

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

- ☐ a. L'*Enrollment* prevede una fase di *feature extraction*.
- ☐ b. L'*Enrollment* prevede una fase di *signal processing*.
- ☒ c. Nessuna delle altre tre scelte. ✓
- ☐ d. L'architettura del processo di *Enrollment* realizza un flusso di esecuzione di tipo iterativo.

Risposta corretta.

La risposta corretta è:

Nessuna delle altre tre scelte.

Domanda 15

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

- ☒ a. In un certificato *self-signed* il valore del campo *Issuer* coincide col valore del campo *Subject* della CA che lo ha emesso. ✗
- ☐ b. Nessuna delle altre tre scelte

MacBook Pro

Domanda 7

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

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

Risposta errata.

La risposta corretta è:

Nessuna delle altre tre scelte.

Domanda 8

Risposta
corretta

Punteggio
ottenuto 1 su 1



Contrassegna
domanda

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

- ☐ a. `openssl pkey -in keyA.pem -out pubA.pem`
- ☒ b. `openssl pkey -in keyA.pem -pubout -out pubA.pem` ✓

Nessuna delle altre tre scelte.

Domanda 15

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

- ☒ a. In un certificato *self-signed* il valore del campo *Issuer* coincide col valore del campo *Subject* della CA che lo ha emesso. ✗
- ☐ b. Nessuna delle altre tre scelte.
- ☐ c. In un certificato *self-signed* il valore del campo *Issuer* coincide col valore del campo *Subject*.
- ☐ d. In un certificato *self-signed* il valore del campo *Issuer* è diverso dal valore del campo *Subject*.

Risposta errata.

La risposta corretta è:

In un certificato *self-signed* il valore del campo *Issuer* coincide col valore del campo *Subject*.

Domanda 16

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

- ☐ a. La sessione deve appartenere allo stesso processo che l'ha creata.
- ☐ b. SSL/TLS consentono di rinegoziare i parametri

MacBook Pro

Domanda 9

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

- ☐ a. L'analisi dinamica black box rappresenta un approccio superficiale per la comprensione di un malware.
- ☐ b. L'analisi dinamica white box non può portare all'infezione del sistema su cui essa viene effettuata.
- ☐ c. Nessuna delle altre tre scelte.
- ☒ d. L'analisi dinamica consiste nell'esaminare un malware prima della sua esecuzione. ✖

Risposta errata.

La risposta corretta è:

L'analisi dinamica black box rappresenta un approccio superficiale per la comprensione di un malware.

Domanda 10

Risposta errata

Punteggio

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

MacBook Pro

Domanda 13

Risposta
corretta

Punteggio
ottenuto 2 su 2



Contrassegna
domanda

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

In un cifrario di Feistel l'i-esima iterazione può essere descritta come

- ☐ a. $L_{i+1} = R_i$ e $R_{i+1} = L_i \text{ XOR } f(L_i, K_{i+1})$
- ☒ b. $L_{i+1} = R_i$ e $R_{i+1} = L_i \text{ XOR } f(R_i, K_{i+1})$ ✓
- ☐ c. $L_{i+1} = R_i \text{ XOR } L_i$ e $R_{i+1} = L_i \text{ XOR } f(R_i, K_{i+1})$
- ☐ d. $L_{i+1} = R_i$ e $R_{i+1} = L_i \text{ XOR } f(L_i \text{ XOR } R_i, K_{i+1})$

Risposta corretta.

La risposta corretta è:

$L_{i+1} = R_i$ e $R_{i+1} = L_i \text{ XOR } f(R_i, K_{i+1})$

Domanda 14

Risposta
corretta

Punteggio
ottenuto 2 su 2



Contrassegna
domanda

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

- ☐ a. L'Enrollment prevede una fase di *feature extraction*.
- ☐ b. L'Enrollment prevede una fase di *signal processing*.
- ☒ c. Nessuna delle altre tre scelte. ✓

Risposta corretta.

La risposta corretta è:

Nessuna delle altre tre scelte.

Domanda 20

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

Indicare quale tra le seguenti affermazioni è corretta.

È possibile effettuare una sola scelta:

- ☒ a. Nessuna delle altre tre scelte. ✗
- ☐ b. Utilizzando Base64 per codificare la stringa binaria
01000001010000100100001101000100 sono necessari 6 caratteri stampabili.
- ☐ c. Utilizzando Base64 per codificare la stringa binaria
01000001010000100100001101000100 sono necessari 8 caratteri stampabili.
- ☐ d. Utilizzando Base64 per codificare la stringa binaria
01000001010000100100001101000100 sono necessari 7 caratteri stampabili.

Risposta errata.

La risposta corretta è:

Utilizzando Base64 per codificare la stringa binaria
01000001010000100100001101000100 sono necessari 8 caratteri stampabili.

MacBook Pro

che l'ha creata.

Domanda 17

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

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

- ☐ a. Nessuna S-box del DES è una funzione lineare dell'input.
- ☐ b. Ogni S-box del DES è una funzione lineare definita tramite un polinomio.
- ☒ c. Le altre tre scelte sono tutte sbagliate. ✗
- ☐ d. Ogni S-box del DES è una funzione lineare, facile da calcolare e difficile da invertire.

Risposta errata.

La risposta corretta è:

Nessuna S-box del DES è una funzione lineare dell'input.

Domanda 18

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

- ☐ a. È possibile effettuare il "resume" di una sessione in base al valore del campo *client_version*.

☐ b. Nessuna delle altre tre scelte.

Risposta errata.

La risposta corretta è:

In un certificato *self-signed* il valore del campo *Issuer* coincide col valore del campo *Subject*.

Domanda **16**

Risposta errata

Punteggio
ottenuto 0 su 1



Contrassegna
domanda

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

- ☐ a. La sessione deve appartenere allo stesso processo che l'ha creata.
- ☐ b. SSL/TLS consentono di rinegoziare i parametri SSL/TLS senza interrompere la connessione.
- ☒ c. Nessuna delle altre tre scelte. ✗
- ☐ d. SSL/TLS consentono di mantenere una sessione attiva dopo aver chiuso una connessione.

Risposta errata.

La risposta corretta è:

La sessione deve appartenere allo stesso processo che l'ha creata.

Domanda **17**

Risposta errata

Punteggio
ottenuto 0 su 2

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

Domanda 12

Risposta
corretta

Punteggio
ottenuto 1 su 1



Contrassegna
domanda

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

- ☒ a. La firma digitale può essere utilizzata per garantire confidenzialità. ✓
- ☐ b. La firma digitale può essere utilizzata per garantire autenticazione.
- ☐ c. La firma digitale può essere utilizzata per garantire non ripudio.
- ☐ d. La firma digitale può essere utilizzata per garantire integrità.

Risposta corretta.

La risposta corretta è:

La firma digitale può essere utilizzata per garantire confidenzialità.

Domanda 13

Risposta
corretta

Punteggio
ottenuto 2 su 2



Contrassegna
domanda

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

In un cifrario di Feistel l'i-esima iterazione può essere descritta come

- ☐ a. $L_{i+1} = R_i$ e $R_{i+1} = L_i \text{ XOR } f(L_i, K_{i+1})$
- ☒ b. $L_{i+1} = R_i$ e $R_{i+1} = L_i \text{ XOR } f(R_i, K_{i+1})$ ✓
- ☐ c. $L_{i+1} = R_i \text{ XOR } L_i$ e $R_{i+1} = L_i \text{ XOR } f(L_i, K_{i+1})$

La risposta corretta è:

$p = 5$ e $g = 2$.

Domanda 11

Risposta errata

Punteggio
ottenuto 0 su 2



Contrassegna
domanda

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

- ☐ a. `openssl enc -aes-256-cbc -in FileInChiaro -out FileCifrato -e -base64 -pass pass:P1pp0B4ud0`
- ☒ b. `openssl enc -base64 -in FileInChiaro -out FileCifrato` ✗
- ☐ c. Nessuna delle altre tre scelte
- ☐ d. `openssl enc -aes-256-cbc -in FileInChiaro -out Base64 -e`

Risposta errata.

La risposta corretta è:

`openssl enc -aes-256-cbc -in FileInChiaro -out Base64 -e`

Domanda 12

Risposta
corretta

Punteggio

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

- ☒ a. La firma digitale può essere utilizzata per ✓