MODULO 1

UNITÀ 1: LO SCAMBIO A DISTANZA DELLE INFORMAZIONI

Quesiti a scelta multipla

1) b
2) c
3) a
4) a
5) c

Quesiti VERO/FALSO

1) VERO
2) VERO
3) FALSO
4) VERO
5) FALSO
6) VERO

UNITÀ 2: INTRODUZIONE ALLA SICUREZZA INFORMATICA

Quesiti a risposta multipla

1) a
2) d
3) b
4) c

Quesiti VERO/FALSO

1) VERO
2) VERO
3) FALSO
4) FALSO
5) VERO

UNITÀ 3: CRITTOGRAFIA SIMMETRICA

Quesiti a risposta multipla

1) a
2) c
3) b
4) a

Quesiti Vero/falso

1) VERO
2) VERO
3) VERO
4) FALSO
5) VERO

Quesiti a completamento

1) L'attacco a forza bruta cerca ogni possibile CHIAVE su un frammento di testo CIFRATO finché non riesce a ottenere una TRADUZIONE corretta.

2) Nel caso l'algoritmo di CIFRATURA elabori un blocco di dati alla VOLTA e per ciascuno di essi fornisca il CORRISPONDENTE blocco di output, la cifratura è detta a BLOCCHI.

3) L'Analisi crittografica è un ATTACCO che si basa sulla conoscenza dell' ALGORITMO di cifratura per tentare di INDIVIDUARE la relativa CHIAVE.

4) Un crittosistema deve essere SICURO anche se il suo funzionamento è di PUBBLICO DOMINIO, con l'eccezione della CHIAVE.

5) Un crittosistema è detto incondizionatamente sicuro se il testo cifrato non CONTIENE informazioni sufficienti per RICOSTRUIRE in modo univoco il TESTO IN CHIARO da cui deriva, indipendentemente dalla quantità di TESTO CIFRATO disponibile.

UNITÀ 4: CIFRARI SIMMETRICI MODERNI

Quesiti a risposta multipla

1) b
2) d
3) a
4) c
5) a

Quesiti a VERO/FALSO

1) VERO
2) VERO
3) VERO
4) VERO
5) FALSO
6) VERO
7) FALSO

UNITÀ 5: CRITTOGRAFIA A CHIAVE PUBBLICA

Quesiti a VERO/FALSO

1) VERO
2) VERO
3) FALSO
4) VERO
5) FALSO
6) VERO

Quesiti a completamento

1) Un utente che vuole comunicare con un altro deve cifrare il messaggio con la chiave pubblica del DESTINATARIO, il quale una volta ricevuto il MESSAGGIO dovrà decifrarlo con la chiave SEGRETA PERSONALE.

2) Per un estraneo deve risultare computazionalmente IMPOSSIBILE, conoscendo la chiave PUBBLICA e il testo CIFRATO, rigenerare il MESSAGGIO ORIGINALE.

3) La bontà di un algoritmo di CRITTOGRAFIA a chiave pubblica dipende dalla individua-zione della funzione TRAPDOORONE-WAY più idonea.

4) Le dimensioni delle chiavi che renderebbero IMPOSSIBILI gli attacchi a forza bruta rendono troppo LENTE le funzionalità della CRITTOGRAFIA.

UNITÀ 6: CIFRARIO RSA

Quesiti a risposta aperta

1) c
2) b
3) a
4) d
5) b

Quesiti VERO/FALSO

1) VERO
2) VERO
3) FALSO
4) VERO
5) FALSO

UNITÀ 7: AUTENTICAZIONE DEI MESSAGGI E FIRMA DIGITALE

Quesiti a risposta multipla

1) a
2) c
3) b
4) d
5) a

Quesiti VERO/FALSO

1) FALSO
2) VERO
3) VERO
4) VERO
5) VERO
6) FALSO
7) VERO

MODULO 2: SICUREZZA DELLE RETI

UNITÀ 1: SICUREZZA DEI SISTEMI INFORMATICI

Quesiti a risposta multipla

1) a
2) d
3) b
4) b
5) c
6) a
7) c

Quesiti VERO/FALSO

1) VERO
2) VERO
3) FALSO
4) VERO
5) VERO
6) VERO
7) FALSO
8) FALSO
9) FALSO

UNITÀ 2: PROTOCOLLI DI PREVENZIONE A LIVELLO DI APPLICAZIONE

Quesiti a risposta multipla

1) d
2) b
3) a
4) c
5) b

Quesiti VERO/FALSO

1) VERO
2) VERO
3) FALSO
4) VERO
5) VERO
6) VERO

Quesiti a completamento

1) Un certificato digitale è un file contenente alcuni dati IDENTIFICATIVI DELL'UTENTE abbinati alla sua CHIAVE PUBBLICA, controfirmato da una o più AUTORITÀ DI CERTIFICAZIONE.

2) L'X509 utilizza la crittografia a CHIAVE PUBBLICA e la FIRMA DIGITALE, ma non prevede l'uso di un algoritmo particolare, anche se è vivamente consigliato l'impiego di RSA.

3) Una directory è un SERVER in grado di gestire un DATABASE di informazioni dei propri utenti, che include un MAPPING fra il nome utente e L'INDIRIZZO DI RETE e/o altri attributi.

4) Kerberos è un protocollo di AUTENTICAZIONE DISTRIBUITO che consente ad un utente di provare la sua IDENTITÀ.

UNITÀ 3: PROTOCOLLI DI PREVENZIONE A LIVELLO DI SESSIONE E DI RETE

Quesiti a risposta multipla

1) a
2) b
3) d
4) c
5) a
6) c

Quesiti VERO/FALSO

1) VERO
2) FALSO
3) VERO
4) VERO
5) FALSO
6) VERO

UNITÀ 4: FIREWALL

Quesiti a risposta multipla

1) b
2) a
3) d
4) b
5) c

Quesiti VERO/FALSO

1) VERO
2) FALSO
3) VERO
4) VERO
5) VERO
6) VERO
7) FALSO

Quesiti a completamento

1) Un packet filter firewall analizza ogni PACCHETTO che lo attraversa singolarmente, senza tenere conto di quelli che lo hanno PRECEDUTO.

2) Il NAT consente di NASCONDERE dietro un unico indirizzo PUBBLICO più i indirizzi PRIVATI.

3) Se un pacchetto appartiene ad una delle CONNESSIONI contenute nella TABELLA DI STATO, viene fatto PASSARE, altrimenti viene BLOCCATO.

4) Il firewall come una DOGANA che controlla tutto il TAFFICO DATI che proviene sia dall'INTERNO sia dall'ESTERNO di una data rete, lasciando passare solo tutto ciò che rispetta le REGOLE.

5) La tipologia di funzionamento state full packet inspection verifica lo STATO della connessione in CORSO e quindi assicura che il DESTINATARIO abbia effettivamente richiesto quella CONNESIONE.

UNITÀ 5: SICUREZZA NELLE WIRELESS LAN

Quesiti a risposta multipla

1) d
2) b
3) a
4) c
5) b

Quesiti VERO/FALSO

1) FALSO
2) FALSO
3) VERO
4) VERO
5) VERO
6) VERO

UNITA 6: SOFTWARE DOLOSI

Quesiti VERO/FALSO

1) VERO
2) VERO
3) VERO
4) FALSO
5) VERO
6) VERO

Quesiti a risposta multipla

1) La trap door viene attivata dal PROGRAMMATORE tramite un particolare CODICE UTENTE.

2) I cavalli di Troia vengono in genere utilizzati per svolgere INDIRETTAMENTE delle funzioni che un utente non autorizzato non potrebbe svolgere DIRETTAMENTE.

3) Gli Zombie vengono utilizzati per effettuare attacchi DENIAL OF SERVICE, normalmente contro SITI WEB.

4) La maggior parte dei virus giunge attraverso la rete INTERNET mediante la POSTA ELETTRONICA.

5) Un worm è un tipo di PROGRAMMA MALEVOLO la cui caratteristica è quello di infiltrarsi sui COMPUTER per poi propagarsi in maniera tale da DIFFONDERSI ad altri computer, sfruttando le capacità di COMUNICAZIONE della rete (Internet, contatti e-mail).

6) La caratteristica peculiare degli worm è di INFETTARE senza la necessità dell'interazione con l' UTENTE.