



Home > My courses > PROG. IK REGULAR > REG - Gasal 2020/2021 > [Reg] Jaringan Komputer (A,B,C) Gasal 2020-2021 > 8. Security in Computer Networks
> Quiz: Wireless + Security

Started on Wednesday, 30 December 2020, 8:00 PM

State Finished

Completed on Wednesday, 30 December 2020, 8:29 PM

Time taken 28 mins 53 secs

Marks 14.00/25.00

Grade 56.00 out of 100.00

Question 1

Correct

Mark 1.00 out of 1.00

Sebuah perusahaan menggunakan solusi IoT untuk monitoring proses manufakturnya. Perangkat IoT tersebut berkomunikasi dengan base station jaringan seluler 4G. Contoh ini masuk dalam kategori wireless dengan mode multi-hop dan infrastructure.

Select one:

- ☐ True
- ☒ False ✓

It is an infrastructure mode but there is only one hop: IoT device directly to base station

The correct answer is 'False'.

Question 2

Correct

Mark 1.00 out of 1.00

Interferensi pada sistem wireless diakibatkan oleh transmisi yang dilakukan oleh wireless node lain yang menggunakan frequency band yang sama.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Question 3

Correct

Mark 1.00 out of 1.00

Wireless host hanya dapat menggunakan satu teknik modulasi (e.g. BPSK). Jika pada satu saat SNR yang diterima host tersebut berkurang, maka BER akan semakin kecil.

Select one:

- ☐ True
- ☒ False ✓

Smaller SNR leads to higher BER (and vice versa), assuming only one modulation scheme is used

The correct answer is 'False'.

Question 4

Incorrect

Mark 0.00 out of 1.00

Standard WiFi berikut tidak bekerja pada frequency band 2.4 GHz:

Select one:

- ☐ a. 802.11ac
- ☐ b. 802.11g
- ☒ c. 802.11ax ✗
- ☐ d. 802.11n

Your answer is incorrect.

The correct answer is: 802.11ac

Question 5

Correct

Mark 1.00 out of 1.00

Standard WiFi berikut memiliki data rate maximum di atas 1 Gbps:

Select one:

- ☐ a. 802.11a
- ☒ b. 802.11ac ✓
- ☐ c. 802.11n
- ☐ d. 802.11g

Your answer is correct.

The correct answer is: 802.11ac

Question 6

Incorrect

Mark 0.00 out of 1.00

Adi dan Bagas sedang nongkrong di sebuah cafe dan keduanya ingin mengakses internet menggunakan WiFi. Adi ingin menggunakan WiFi yang disediakan oleh cafe, sedangkan Bagas ingin menggunakan WiFi hotspot nya sendiri (e.g. modem 4G WiFi). Hotspot yang disetup Bagas menggunakan channel yang berbeda dengan access point WiFi milik cafe (hotspot Bagas pada channel 1 dan access point cafe pada channel 11). Pada kasus ini, akan terjadi collision jika kedua gawai Adi dan Bagas transmit ke access point masing-masing secara bersamaan.

Select one:

- ☒ True ✖
- ☐ False

Both of them can transmit at the same time because they are operating in different channel, thus no collision.

The correct answer is 'False'.

Question 7

Incorrect

Mark 0.00 out of 1.00

Sebuah WiFi host dengan protokol multiple access CSMA/CA akan segera menghentikan transmisi ketika host tersebut mendeteksi adanya packet collision.

Select one:

- ☒ True ✖
- ☐ False

Ability to detect collision and abort transmission when a collision is detected belongs to CSMA/CD

The correct answer is 'False'.

Question 8

Incorrect

Mark 0.00 out of 1.00

Radio Network Controller (RNC) pada jaringan 3G mengendalikan atau melayani beberapa BTS, dan juga memisahkan traffic voice dan traffic data.

Select one:

- ☐ True
- ☒ False ✖

The correct answer is 'True'.

Question 9

Correct

Mark 1.00 out of 1.00

Traffic voice dan traffic data dibuat terpisah pada jaringan LTE.

Select one:

- ☐ True
- ☒ False ✓

Voice traffic and data traffic are separated in 2.5G (GPRS) and 3G networks. But 4G LTE has unified architecture, i.e. all IP network architecture for all kinds of traffic (including voice and data)

The correct answer is 'False'.

Question 10

Correct

Mark 1.00 out of 1.00

Replay atau playback attack dapat dicegah dengan menggunakan MAC dan enkripsi message.

Select one:

- ☐ True
- ☒ False ✓

Replay attack can be prevented by using nonce

The correct answer is 'False'.

Question 11

Incorrect

Mark 0.00 out of 1.00

Agar client yang menggunakan SSL dapat di autentikasi, client tersebut harus memberikan certificate nya ke server.

Select one:

- ☐ True
- ☒ False ✗

The correct answer is 'True'.

Question 12

Correct Mark 7.00 out of 7.00

Tentukan istilah/terminologi paling tepat pada setiap statement berikut:

Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message.

Confidentiality



Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan.

Availability



Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target.

Spoofing



Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi.

Authentication



Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan)

Integrity



Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc).

Distributed Denial of Service



Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker.

Hijacking



Your answer is correct.

The correct answer is: Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message. → Confidentiality, Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan. → Availability, Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target. → Spoofing, Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi. → Authentication, Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan) → Integrity, Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc). → Distributed Denial of Service, Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker. → Hijacking

Question 13

Partially correct

Mark 1.00 out of 7.00

Cocokkanlah tujuan dari solusi cryptography berikut dengan notasi cryptography yang sesuai. Definisi dari notasi cryptography adalah sebagai berikut:

- m = message
- K_s = Symmetric key
- K_{s+} = Sender's public key
- K_{s-} = Sender's private key
- K_{r+} = Receiver's public key
- K_{r-} = Receiver's private key
- $H(m)$ = hashed of a message
- MAC = Message Authentication Code

Menjamin

integritas dan

authenticity

sebuah message

Sender: $K_{r+}(m)$; Receiver: $K_{r-}(K_{r+}(m))$

menggunakan ✖

public key

cryptography

Menjamin

kerahasiaan

sebuah message

Sender: $K_{r+}(m)$; Receiver: $K_{r-}(K_{r+}(m))$

menggunakan ✔

public key

cryptography

Menjamin

integritas dan

authenticity

sebuah message

Sender: $K_{r+}(m)$; Receiver: $K_{r-}(K_{r+}(m))$

dengan message ✖

digest dan

public key

cryptography

Menjamin

kerahasiaan,

integritas dan

authenticity

sebuah message

Sender: $K_{r+}(m)$; Receiver: $K_{r-}(K_{r+}(m))$

menggunakan

message digest ✖

serta kombinasi

symmetric dan

public key

cryptography

Menjamin
integritas dan
authenticity
sebuah message
menggunakan
symmetric key
cryptography

Sender: $Kr+(m)$; Receiver: $Kr-(Kr+(m))$

Menjamin
kerahasiaan,
integritas dan
authenticity
sebuah message
menggunakan
kombinasi
symmetric dan
public key
cryptography

Sender: $Kr+(m)$; Receiver: $Kr-(Kr+(m))$

Menjamin
kerahasiaan
sebuah message
menggunakan
kombinasi
symmetric dan
public key
cryptography

Sender: $Kr+(m)$; Receiver: $Kr-(Kr+(m))$

Your answer is partially correct.

You have correctly selected 1.

The correct answer is: Menjamin integritas dan authenticity sebuah message menggunakan public key cryptography → Sender: $m, Ks-(m)$; Receiver: $verify(m = Ks+(Ks-(m)))$, Menjamin kerahasiaan sebuah message menggunakan public key cryptography → Sender: $Kr+(m)$; Receiver: $Kr-(Kr+(m))$, Menjamin integritas dan authenticity sebuah message dengan message digest dan public key cryptography → Sender: $m, Ks-(H(m))$; Receiver: $H(m), verify(H(m) = Ks+(Ks-(H(m))))$, Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan message digest serta kombinasi symmetric dan public key cryptography → Sender: $Ks(m, Ks-(H(m)))$, $Kr+(Ks)$; Receiver: $Kr-(Kr+(Ks))$, $Ks(Ks(m, Ks-(m))), H(m), verify(m = Ks+(Ks-(m)))$, Menjamin integritas dan authenticity sebuah message menggunakan symmetric key cryptography → $MAC(Ks, m)$, Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: $Ks(m, Ks-(m))$, $Kr+(Ks)$; Receiver: $Kr-(Kr+(Ks))$, $Ks(Ks(m, Ks-(m))), verify(m = Ks+(Ks-(m)))$, Menjamin kerahasiaan sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: $Ks(m), Kr+(Ks)$; Receiver: $Kr-(Kr+(Ks))$, $Ks(Ks(m))$



Home > My courses > PROG. IK REGULAR > REG - Gasal 2020/2021 > [Reg] Jaringan Komputer (A,B,C) Gasal 2020-2021 > 8. Security in Computer Networks
> Quiz: Wireless + Security

Started on Wednesday, 30 December 2020, 8:03 PM

State Finished

Completed on Wednesday, 30 December 2020, 8:32 PM

Time taken 29 mins 50 secs

Marks 18.00/25.00

Grade 72.00 out of 100.00

Question 1

Incorrect

Mark 0.00 out of 1.00

Sistem smart home menggunakan teknologi Zigbee untuk mengendalikan perangkat rumah tangga secara wireless (seperti remote control). Selain itu, sistem tersebut juga menggunakan multi-hop routing sehingga remote control dapat menggapai perangkat yang tidak berada dalam jangkauannya. Contoh tersebut masuk dalam kategori wireless dalam mode multi-hop dan infrastructure.

Select one:

- ☒ True ✖
- ☐ False

It is an adhoc multi-hop mode, because it only wants to control the appliances within the home, not through internet.

The correct answer is 'False'.

Question 2

Correct

Mark 1.00 out of 1.00

Atenuasi pada signal wireless terjadi karena noise dari sumber internal dan external.

Select one:

- ☐ True
- ☒ False ✔

Signal attenuation happens due to longer distance or obstacles between transmitter and receiver, while noise contributes to the SNR value (denominator to the signal power).

The correct answer is 'False'.



Question 3

Correct

Mark 1.00 out of 1.00

Multipath propagation pada kanal wireless diakibatkan oleh gelombang electromagnetic yang dipantulkan oleh beberapa benda atau permukaan antara transmitter dan receiver, sehingga ada beberapa versi sinyal (dalam hal waktu tiba dan signal power) yang tiba di receiver.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Question 4

Correct

Mark 1.00 out of 1.00

Standard WiFi berikut menggunakan OFDMA sebagai protokol multiple access:

Select one:

- ☐ a. 802.11a
- ☐ b. 802.11ac
- ☐ c. 802.11n
- ☒ d. 802.11ax ✓

Your answer is correct.

The correct answer is: 802.11ax

Question 5

Correct

Mark 1.00 out of 1.00

Standard WiFi berikut memiliki data rate maximum di atas 1 Gbps:

Select one:

- ☐ a. 802.11n
- ☒ b. 802.11ac ✓
- ☐ c. 802.11a
- ☐ d. 802.11g

Your answer is correct.

The correct answer is: 802.11ac



Question 6

Correct

Mark 1.00 out of 1.00

Adi dan Bagas sedang nongkrong di sebuah cafe dan keduanya ingin mengakses internet menggunakan WiFi. Adi ingin menggunakan WiFi yang disediakan oleh cafe, sedangkan Bagas ingin menggunakan WiFi hotspot nya sendiri (e.g. modem 4G WiFi). Kebetulan, hotspot yang disetup Bagas menggunakan channel yang sama dengan access point WiFi milik cafe. Pada kasus ini, gawai Adi dan Bagas tidak akan dapat berasosiasi dan berkomunikasi dengan Access Point tujuan mereka masing-masing (asumsi mereka tidak transmit pada saat bersamaan).

Select one:

- ☐ True
- ☒ False ✓

Both of them can still associate to different access points although the access points operate in the same channel/frequency. They can also communicate with their respective access point, as long as they are not transmitting at the same time (concurrent transmission in the same channel leads to collision).

The correct answer is 'False'.

Question 7

Correct

Mark 1.00 out of 1.00

Sebuah WiFi host dengan mekanisme *Collision Avoidance* akan melakukan sensing terhadap medium terlebih dahulu sebelum mengirim frame. Host tersebut hanya akan mengirim frame jika medium idle selama beberapa saat yang sudah ditetapkan.

Select one:

- ☐ True
- ☒ False ✓

WiFi with collision avoidance will first make sure that there is no hidden terminal by using RTS-CTS mechanism

The correct answer is 'False'.

Question 8

Correct

Mark 1.00 out of 1.00

Traffic voice dan traffic data dibuat terpisah pada jaringan LTE.

Select one:

- ☐ True
- ☒ False ✓

Voice traffic and data traffic are separated in 2.5G (GPRS) and 3G networks. But 4G LTE has unified architecture, i.e. all IP network architecture for all kinds of traffic (including voice and data)

The correct answer is 'False'.




Question 9

Incorrect

Mark 0.00 out of 1.00

Jaringan GSM menggunakan kombinasi FDMA dan TDMA untuk protokol multiple access. Hal itu berarti users yang ada di cell yang sama akan menggunakan frekuensi berbeda untuk berkomunikasi dengan base station di cell tersebut.

Select one:

- ☒ True 
- ☐ False

Different frequencies are used for Base stations in the neighboring cells, so that they do not interfere to each other. It means that the base station in a particular cell uses a single frequency (unless the base station uses sectoral antenna, assigning different frequency in different sector), and that frequency is shared by users in that cell. Multiple users within the same cell are assigned with different time slot to communicate with the base station (TDMA).

The correct answer is 'False'.


Question 10

Correct

Mark 1.00 out of 1.00

Algoritma DES membutuhkan public key dan private key, sedangkan algoritma RSA hanya digunakan untuk enkripsi.

Select one:

- ☐ True
- ☒ False 

DES is symmetric key, so it has no public-private key pair. RSA can also be used to create digital signature

The correct answer is 'False'.


Question 11

Correct

Mark 1.00 out of 1.00

Fungsi hash menghasilkan output dengan panjang byte yang fix.

Select one:

- ☒ True 
- ☐ False

The correct answer is 'True'.



Question 12

Partially correct

Mark 6.00 out of 7.00

Tentukan istilah/terminologi paling tepat pada setiap statement berikut:

Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker.

Hijacking



Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc).

Distributed Denial of Service



Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message.

Confidentiality



Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target.

Spoofing



Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi.

Authorization



Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan.

Availability



Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan)

Integrity



Your answer is partially correct.

You have correctly selected 6.

The correct answer is: Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker. → Hijacking, Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc). → Distributed Denial of Service, Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message. → Confidentiality, Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target. → Spoofing, Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi. → Authentication, Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan. → Availability, Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan) → Integrity



Question 13

Partially correct

Mark 3.00 out of 7.00

Cocokkanlah tujuan dari solusi cryptogaphy berikut dengan notasi cryptography yang sesuai. Definisi dari notasi cryptography adalah sebagai berikut:

- m = message
- K_s = Symmetric key
- K_{s+} = Sender's public key
- K_{s-} = Sender's private key
- K_{r+} = Receiver's public key
- K_{r-} = Receiver's private key
- $H(m)$ = hashed of a message
- MAC = Message Authentication Code

Menjamin

kerahasiaan

sebuah message

menggunakan

Sender: $m, K_{s-}(m)$; Receiver: $\text{verify}(m = K_{s+}(K_{s-}(m)))$

kombinasi



symmetric dan

public key

cryptography

Menjamin

integritas dan

authenticity

sebuah message

Sender: $K_s(m, K_{r+}(m)), K_{s-}(K_s)$; Receiver: $K_{s+}(K_{s-}(K_s)), K_s(K_s(m, K_{r+}(m)))$, $\text{verify}(m = K_{r-}(K_{r+}(m)))$

dengan message



digest dan

public key

cryptography

Menjamin

kerahasiaan,

integritas dan

authenticity

sebuah message

Sender: $K_s(m, K_{s-}(m)), K_{r+}(K_s)$; Receiver: $K_{r-}(K_{r+}(K_s)), K_s(K_s(m, K_{s-}(m)))$, $\text{verify}(m = K_{s+}(K_{s-}(m)))$

menggunakan



kombinasi

symmetric dan

public key

cryptography

Menjamin

integritas dan

authenticity

sebuah message

Sender: $m, K_{s-}(m)$; Receiver: $\text{verify}(m = K_{s+}(K_{s-}(m)))$

menggunakan



public key

cryptography



Menjamin
integritas dan
authenticity
sebuah message
menggunakan
symmetric key
cryptography

Sender: $m, K_s(m)$; Receiver: $\text{verify}(m = K_s(K_s(m)))$

Menjamin
kerahasiaan
sebuah message
menggunakan
public key
cryptography

Sender: $K_r(m)$; Receiver: $K_r(K_r(m))$

Menjamin
kerahasiaan,
integritas dan
authenticity
sebuah message
menggunakan
message digest
serta kombinasi
symmetric dan
public key
cryptography

Sender: $m, K_s(H(m))$; Receiver: $H(m), \text{verify}(H(m) = K_s(K_s(H(m))))$

Your answer is partially correct.

You have correctly selected 3.

The correct answer is: Menjamin kerahasiaan sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: $K_s(m), K_r(K_s)$; Receiver: $K_r(K_r(K_s)), K_s(K_s(m))$, Menjamin integritas dan authenticity sebuah message dengan message digest dan public key cryptography → Sender: $m, K_s(H(m))$; Receiver: $H(m), \text{verify}(H(m) = K_s(K_s(H(m))))$, Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: $K_s(m, K_s(m)), K_r(K_s)$; Receiver: $K_r(K_r(K_s)), K_s(K_s(m, K_s(m)), \text{verify}(m = K_s(K_s(m))))$, Menjamin integritas dan authenticity sebuah message menggunakan public key cryptography → Sender: $m, K_s(m)$; Receiver: $\text{verify}(m = K_s(K_s(m)))$, Menjamin integritas dan authenticity sebuah message menggunakan symmetric key cryptography → $\text{MAC}(K_s, m)$, Menjamin kerahasiaan sebuah message menggunakan public key cryptography → Sender: $K_r(m)$; Receiver: $K_r(K_r(m))$, Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan message digest serta kombinasi symmetric dan public key cryptography → Sender: $K_s(m, K_s(H(m))), K_r(K_s)$; Receiver: $K_r(K_r(K_s)), K_s(K_s(m, K_s(m)), H(m), \text{verify}(m = K_s(K_s(m))))$





Home > My courses > PROG. IK REGULAR > REG - Gasal 2020/2021 > [Reg] Jaringan Komputer (A,B,C) Gasal 2020-2021 > 8. Security in Computer Networks
> Quiz: Wireless + Security

Started on Wednesday, 30 December 2020, 8:02 PM

State Finished

Completed on Wednesday, 30 December 2020, 8:24 PM

Time taken 21 mins 55 secs

Marks 16.00/25.00

Grade 64.00 out of 100.00

Question 1

Incorrect Mark 0.00 out of 1.00

Sebuah perusahaan menggunakan solusi IoT untuk monitoring proses manufakturnya. Perangkat IoT tersebut berkomunikasi dengan base station jaringan seluler 4G. Contoh ini masuk dalam kategori wireless dengan mode multi-hop dan infrastructure.

Select one:

- ☒ True ✗
- ☐ False

It is an infrastructure mode but there is only one hop: IoT device directly to base station

The correct answer is 'False'.

Question 2

Correct Mark 1.00 out of 1.00

Interferensi pada sistem wireless diakibatkan oleh transmisi yang dilakukan oleh wireless node lain yang menggunakan frequency band yang sama.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Question 3

Correct

Mark 1.00 out of 1.00

Wireless host hanya dapat menggunakan satu teknik modulasi (e.g. BPSK). Jika pada satu saat SNR yang diterima host tersebut berkurang, maka BER akan semakin kecil.

Select one:

- ☐ True
- ☒ False ✓

Smaller SNR leads to higher BER (and vice versa), assuming only one modulation scheme is used

The correct answer is 'False'.

Question 4

Correct

Mark 1.00 out of 1.00

Standard WiFi berikut tidak bekerja pada frequency band 2.4 GHz:

Select one:

- ☐ a. 802.11g
- ☒ b. 802.11ac ✓
- ☐ c. 802.11ax
- ☐ d. 802.11n

Your answer is correct.

The correct answer is: 802.11ac

Question 5

Correct

Mark 1.00 out of 1.00

Standard WiFi berikut menggunakan OFDMA sebagai protokol multiple access:

Select one:

- ☐ a. 802.11a
- ☐ b. 802.11ac
- ☐ c. 802.11n
- ☒ d. 802.11ax ✓

Your answer is correct.

The correct answer is: 802.11ax

Question 6

Correct

Mark 1.00 out of 1.00

Adi dan Bagas sedang nongkrong di sebuah cafe dan keduanya ingin mengakses internet menggunakan WiFi. Adi ingin menggunakan WiFi yang disediakan oleh cafe, sedangkan Bagas ingin menggunakan WiFi hotspot nya sendiri (e.g. modem 4G WiFi). Kebetulan, hotspot yang disetup Bagas menggunakan channel yang sama dengan access point WiFi milik cafe. Pada kasus ini, gawai Adi dan Bagas tidak akan dapat berasosiasi dan berkomunikasi dengan Access Point tujuan mereka masing-masing (asumsi mereka tidak transmit pada saat bersamaan).

Select one:

- ☐ True
- ☒ False ✓

Both of them can still associate to different access points although the access points operate in the same channel/frequency. They can also communicate with their respective access point, as long as they are not transmitting at the same time (concurrent transmission in the same channel leads to collision).

The correct answer is 'False'.

Question 7

Incorrect

Mark 0.00 out of 1.00

Sebuah WiFi host dengan protokol multiple access CSMA/CA akan segera menghentikan transmisi ketika host tersebut mendeteksi adanya packet collision.

Select one:

- ☒ True ✗
- ☐ False

Ability to detect collision and abort transmission when a collision is detected belongs to CSMA/CD

The correct answer is 'False'.

Question 8

Correct

Mark 1.00 out of 1.00

Jaringan GSM menggunakan kombinasi FDMA dan TDMA sebagai protokol multiple access. Hal itu berarti users yang berada di cell berbeda TIDAK dapat menggunakan timeslot yang sama secara mutlak untuk berkomunikasi dengan base station mereka di cell tersebut.

Select one:

- ☐ True
- ☒ False ✓

Multiple users within the same cell are assigned with different time slot to communicate with the base station (TDMA). But users in different cell may be assigned with the same time slot to communicate with their respective base station, since base station in different cells work independently.

The correct answer is 'False'.

Question 9

Correct

Mark 1.00 out of 1.00

Radio Network Controller (RNC) pada jaringan 3G mengendalikan atau melayani beberapa BTS, dan juga memisahkan traffic voice dan traffic data.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Question 10

Correct

Mark 1.00 out of 1.00

Proses enkripsi atau dekripsi menggunakan asymmetric cryptography lebih lambat daripada symmetric.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.


Question 11

Incorrect

Mark 0.00 out of 1.00

Agar client yang menggunakan SSL dapat di autentikasi, client tersebut harus memberikan certificate nya ke server.

Select one:

- ☐ True
- ☒ False 

The correct answer is 'True'.

Question 12

Partially correct

Mark 6.00 out of 7.00

Tentukan istilah/terminologi paling tepat pada setiap statement berikut:

Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan)

Integrity ▼



Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message.

Authorization ▼



Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target.

Spoofing ▼



Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi.

Authentication ▼



Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan.

Availability ▼



Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc).

Distributed Denial of Service ▼



Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker.

Hijacking ▼



Your answer is partially correct.

You have correctly selected 6.

The correct answer is: Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan) → Integrity, Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message. → Confidentiality, Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target. → Spoofing, Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi. → Authentication, Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan. → Availability, Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc). → Distributed Denial of Service, Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker. → Hijacking

Question 13

Partially correct

Mark 2.00 out of 7.00

Cocokkanlah tujuan dari solusi cryptography berikut dengan notasi cryptography yang sesuai. Definisi dari notasi cryptography adalah sebagai berikut:

- m = message
- K_s = Symmetric key
- K_{s+} = Sender's public key
- K_{s-} = Sender's private key
- K_{r+} = Receiver's public key
- K_{r-} = Receiver's private key
- $H(m)$ = hashed of a message
- MAC = Message Authentication Code

Menjamin

kerahasiaan,

integritas dan

authenticity

sebuah message

menggunakan

kombinasi

symmetric dan

public key

cryptography

Sender: $K_s(m, K_{r+}(m)), K_{s-}(K_s)$; Receiver: $K_{s+}(K_{s-}(K_s)), K_s(K_s(m, K_{r+}(m)))$, verify($m = K_{r-}(K_{r+}(m))$)

Menjamin

integritas dan

authenticity

sebuah message

menggunakan

public key

cryptography

Sender: $m, K_{s-}(H(m))$; Receiver: $H(m)$, verify($H(m) = K_{s+}(K_{s-}(H(m)))$)

Menjamin

integritas dan

authenticity

sebuah message

dengan message

digest dan

public key

cryptography

Sender: $m, K_{s-}(H(m))$; Receiver: $H(m)$, verify($H(m) = K_{s+}(K_{s-}(H(m)))$)

Menjamin

kerahasiaan

sebuah message

menggunakan

kombinasi

symmetric dan

public key

cryptography

Sender: $K_s(m), K_{s-}(K_s)$; Receiver: $K_{s+}(K_{s-}(K_s)), K_s(K_s(m))$

Menjamin
integritas dan
authenticity
sebuah message
menggunakan
symmetric key
cryptography

Sender: $K_s(m)$, $K_r+(K_s)$; Receiver: $K_r-(K_r+(K_s))$, $K_s(K_s(m))$

Menjamin
kerahasiaan,
integritas dan
authenticity
sebuah message
menggunakan
message digest
serta kombinasi
symmetric dan
public key
cryptography

Sender: $K_s(m, K_s-(H(m)))$, $K_r+(K_s)$; Receiver: $K_r-(K_r+(K_s))$, $K_s(K_s(m, K_s-(m)))$, $H(m)$, verify($m = K_s+(K_s-(m))$)

Menjamin
kerahasiaan
sebuah message
menggunakan
public key
cryptography

Sender: $K_s-(m)$; Receiver: $K_s+(K_s-(m))$

Your answer is partially correct.

You have correctly selected 2.

The correct answer is: Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: $K_s(m, K_s-(m))$, $K_r+(K_s)$; Receiver: $K_r-(K_r+(K_s))$, $K_s(K_s(m, K_s-(m)))$, verify($m = K_s+(K_s-(m))$), Menjamin integritas dan authenticity sebuah message menggunakan public key cryptography → Sender: $m, K_s-(m)$; Receiver: verify($m = K_s+(K_s-(m))$), Menjamin integritas dan authenticity sebuah message dengan message digest dan public key cryptography → Sender: $m, K_s-(H(m))$; Receiver: $H(m)$, verify($H(m) = K_s+(K_s-(H(m)))$), Menjamin kerahasiaan sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: $K_s(m), K_r+(K_s)$; Receiver: $K_r-(K_r+(K_s))$, $K_s(K_s(m))$, Menjamin integritas dan authenticity sebuah message menggunakan symmetric key cryptography → MAC(K_s, m), Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan message digest serta kombinasi symmetric dan public key cryptography → Sender: $K_s(m, K_s-(H(m)))$, $K_r+(K_s)$; Receiver: $K_r-(K_r+(K_s))$, $K_s(K_s(m, K_s-(m)))$, $H(m)$, verify($m = K_s+(K_s-(m))$), Menjamin kerahasiaan sebuah message menggunakan public key cryptography → Sender: $K_r+(m)$; Receiver: $K_r-(K_r+(m))$



Home > My courses > [Reg] Jaringan Komputer (A,B,C) Gasal 2020-2021 > 8. Security in Computer Networks > Quiz: Wireless + Security

Started on Wednesday, 30 December 2020, 8:10 PM

State Finished

Completed on Wednesday, 30 December 2020, 8:33 PM

Time taken 23 mins 1 sec

Marks 19.00/25.00

Grade 76.00 out of 100.00

Question 1

Incorrect

Mark 0.00 out of 1.00

Sistem smart home menggunakan teknologi Zigbee untuk mengendalikan perangkat rumah tangga secara wireless (seperti remote control). Selain itu, sistem tersebut juga menggunakan multi-hop routing sehingga remote control dapat menggapai perangkat yang tidak berada dalam jangkauannya. Contoh tersebut masuk dalam kategori wireless dalam mode multi-hop dan infrastructure.

Select one:

- ☒ True ✖
- ☐ False

It is an adhoc multi-hop mode, because it only wants to control the appliances within the home, not through internet.

The correct answer is 'False'.

Question 2

Incorrect

Mark 0.00 out of 1.00

Atenuasi pada signal wireless terjadi karena noise dari sumber internal dan external.

Select one:

- ☒ True ✖
- ☐ False

Signal attenuation happens due to longer distance or obstacles between transmitter and receiver, while noise contributes to the SNR value (denominator to the signal power).

The correct answer is 'False'.

Question 3

Correct

Mark 1.00 out of 1.00

Wireless host hanya dapat menggunakan satu teknik modulasi (e.g. BPSK). Jika pada satu saat SNR yang diterima host tersebut berkurang, maka BER akan semakin kecil.

Select one:

- ☐ True
- ☒ False ✓

Smaller SNR leads to higher BER (and vice versa), assuming only one modulation scheme is used

The correct answer is 'False'.

Question 4

Incorrect

Mark 0.00 out of 1.00

Standard WiFi berikut yang tidak support multiple antenna adalah:

Select one:

- ☐ a. 802.11n
- ☐ b. 802.11ac
- ☒ c. 802.11ax ✗
- ☐ d. 802.11g

Your answer is incorrect.

The correct answer is: 802.11g

Question 5

Correct

Mark 1.00 out of 1.00

Standard WiFi berikut tidak bekerja pada frequency band 2.4 GHz:

Select one:

- ☒ a. 802.11ac ✓
- ☐ b. 802.11g
- ☐ c. 802.11n
- ☐ d. 802.11ax

Your answer is correct.

The correct answer is: 802.11ac

Question 6

Correct

Mark 1.00 out of 1.00

Adi dan Bagas sedang nongkrong di sebuah cafe dan keduanya ingin mengakses internet menggunakan WiFi. Adi ingin menggunakan WiFi yang disediakan oleh cafe, sedangkan Bagas ingin menggunakan WiFi hotspot nya sendiri (e.g. modem 4G WiFi). Hotspot yang disetup Bagas menggunakan channel yang berbeda dengan access point WiFi milik cafe (hotspot Bagas pada channel 1 dan access point cafe pada channel 11). Pada kasus ini, akan terjadi collision jika kedua gawai Adi dan Bagas transmit ke access point masing-masing secara bersamaan.

Select one:

- ☐ True
- ☒ False ✓

Both of them can transmit at the same time because they are operating in different channel, thus no collision.

The correct answer is 'False'.

Question 7

Incorrect

Mark 0.00 out of 1.00

Sebuah WiFi host dengan mekanisme *Collision Avoidance* akan melakukan sensing terhadap medium terlebih dahulu sebelum mengirim frame. Host tersebut hanya akan mengirim frame jika medium idle selama beberapa saat yang sudah ditetapkan.

Select one:

- ☒ True ✗
- ☐ False

WiFi with collision avoidance will first make sure that there is no hidden terminal by using RTS-CTS mechanism

The correct answer is 'False'.

Question 8

Correct

Mark 1.00 out of 1.00

Radio Network Controller (RNC) pada jaringan 3G mengendalikan atau melayani beberapa BTS, dan juga memisahkan traffic voice dan traffic data.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Question 9

Correct Mark 1.00 out of 1.00

Traffic voice dan traffic data dibuat terpisah pada jaringan LTE.

Select one:

- ☐ True
- ☒ False ✓

Voice traffic and data traffic are separated in 2.5G (GPRS) and 3G networks. But 4G LTE has unified architecture, i.e. all IP network architecture for all kinds of traffic (including voice and data)

The correct answer is 'False'.

Question 10

Correct Mark 1.00 out of 1.00

Proses enkripsi atau dekripsi menggunakan asymmetric cryptography lebih lambat daripada symmetric.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Question 11

Correct Mark 1.00 out of 1.00

Fungsi hash menghasilkan output dengan panjang byte yang fix.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Question 12

Correct

Mark 7.00 out of 7.00

Tentukan istilah/terminologi paling tepat pada setiap statement berikut:

Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan)

Integrity ▼



Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message.

Confidentiality ▼



Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi.

Authentication ▼



Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan.

Availability ▼



Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker.

Hijacking ▼



Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc).

Distributed Denial of Service ▼



Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target.

Spoofing ▼



Your answer is correct.

The correct answer is: Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan) → Integrity, Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message. → Confidentiality, Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi. → Authentication, Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan. → Availability, Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker. → Hijacking, Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc). → Distributed Denial of Service, Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target. → Spoofing

Question 13

Partially correct

Mark 5.00 out of 7.00

Cocokkanlah tujuan dari solusi cryptography berikut dengan notasi cryptography yang sesuai. Definisi dari notasi cryptography adalah sebagai berikut:


- m = message
- K_s = Symmetric key
- K_{s+} = Sender's public key
- K_{s-} = Sender's private key
- K_{r+} = Receiver's public key
- K_{r-} = Receiver's private key
- $H(m)$ = hashed of a message
- MAC = Message Authentication Code

Menjamin

integritas dan

authenticity

sebuah message

menggunakan 

public key


cryptography

Sender: $m, K_{s-}(m)$; Receiver: verify($m = K_{s+}(K_{s-}(m))$)

Menjamin

kerahasiaan

sebuah message

menggunakan 

public key


cryptography

Sender: $K_s(m)$; Receiver: $K_{s+}(K_s(m))$

Menjamin

kerahasiaan

sebuah message

menggunakan 

kombinasi

symmetric dan

public key

cryptography


Sender: $K_s(m), K_{r+}(K_s)$; Receiver: $K_{r-}(K_{r+}(K_s)), K_s(K_s(m))$

Menjamin

integritas dan

authenticity

sebuah message

dengan message 

digest dan

public key

cryptography

Sender: $m, K_{s-}(H(m))$; Receiver: $H(m)$, verify($H(m) = K_{s+}(K_{s-}(H(m)))$)

Menjamin
integritas dan
authenticity
sebuah message
menggunakan ✓
symmetric key
cryptography

MAC(Ks, m)

Menjamin
kerahasiaan,
integritas dan
authenticity
sebuah message
menggunakan ✗
kombinasi
symmetric dan
public key
cryptography

Sender: Ks(m), Ks-(Ks) ; Receiver: Ks+(Ks-(Ks)), Ks(Ks(m))

Menjamin
kerahasiaan,
integritas dan
authenticity
sebuah message
menggunakan ✓
message digest
serta kombinasi
symmetric dan
public key
cryptography

Sender: Ks(m, Ks-(H(m))), Kr+(Ks) ; Receiver: Kr-(Kr+(Ks)), Ks(Ks(m, Ks-(m))), H(m), verify(m = Ks+(Ks-(m)))

Your answer is partially correct.

You have correctly selected 5.

The correct answer is: Menjamin integritas dan authenticity sebuah message menggunakan public key cryptography → Sender: m, Ks-(m) ; Receiver: verify(m = Ks+(Ks-(m))), Menjamin kerahasiaan sebuah message menggunakan public key cryptography → Sender: Kr+(m) ; Receiver: Kr-(Kr+(m)), Menjamin kerahasiaan sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: Ks(m), Kr+(Ks) ; Receiver: Kr-(Kr+(Ks)), Ks(Ks(m)), Menjamin integritas dan authenticity sebuah message dengan message digest dan public key cryptography → Sender: m, Ks-(H(m)) ; Receiver: H(m), verify(H(m) = Ks+(Ks-(H(m)))), Menjamin integritas dan authenticity sebuah message menggunakan symmetric key cryptography → MAC(Ks, m), Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: Ks(m, Ks-(m)), Kr+(Ks) ; Receiver: Kr-(Kr+(Ks)), Ks(Ks(m, Ks-(m))), verify(m = Ks+(Ks-(m))), Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan message digest serta kombinasi symmetric dan public key cryptography → Sender: Ks(m, Ks-(H(m))), Kr+(Ks) ; Receiver: Kr-(Kr+(Ks)), Ks(Ks(m, Ks-(m))), H(m), verify(m = Ks+(Ks-(m)))



Home > My courses > PROG. IK REGULAR > REG - Gasal 2020/2021 > [Reg] Jaringan Komputer (A,B,C) Gasal 2020-2021 > 8. Security in Computer Networks
> Quiz: Wireless + Security

Started on	Wednesday, 30 December 2020, 8:02 PM
State	Finished
Completed on	Wednesday, 30 December 2020, 8:32 PM
Time taken	30 mins 1 sec
Marks	18.00/25.00
Grade	72.00 out of 100.00

Question 1

Incorrect

Mark 0.00 out of 1.00

Sistem smart home menggunakan teknologi Zigbee untuk mengendalikan perangkat rumah tangga secara wireless (seperti remote control). Selain itu, sistem tersebut juga menggunakan multi-hop routing sehingga remote control dapat menggapai perangkat yang tidak berada dalam jangkauannya. Contoh tersebut masuk dalam kategori wireless dalam mode multi-hop dan infrastructure.

Select one:

- ☒ True ✗
- ☐ False

It is an adhoc multi-hop mode, because it only wants to control the appliances within the home, not through internet.
The correct answer is 'False'.

Question 2

Correct

Mark 1.00 out of 1.00

Wireless host hanya dapat menggunakan satu teknik modulasi (e.g. BPSK). Jika pada satu saat SNR yang diterima host tersebut berkurang, maka BER akan semakin kecil.

Select one:

- ☐ True
- ☒ False ✓

Smaller SNR leads to higher BER (and vice versa), assuming only one modulation scheme is used
The correct answer is 'False'.

Question 3

Correct

Mark 1.00 out of 1.00

Atenuasi pada signal wireless terjadi karena noise dari sumber internal dan external.

Select one:

- ☐ True
- ☒ False ✓

Signal attenuation happens due to longer distance or obstacles between transmitter and receiver, while noise contributes to the SNR value (denominator to the signal power).

The correct answer is 'False'.

Question 4

Correct

Mark 1.00 out of 1.00

Standard WiFi berikut tidak bekerja pada frequency band 2.4 GHz:

Select one:

- ☒ a. 802.11ac ✓
- ☐ b. 802.11g
- ☐ c. 802.11n
- ☐ d. 802.11ax

Your answer is correct.

The correct answer is: 802.11ac

Question 5

Correct

Mark 1.00 out of 1.00

Standard WiFi berikut memiliki data rate maximum di atas 1 Gbps:

Select one:

- ☐ a. 802.11g
- ☐ b. 802.11n
- ☐ c. 802.11a
- ☒ d. 802.11ac ✓

Your answer is correct.

The correct answer is: 802.11ac

Adi dan Bagas sedang nongkrong di sebuah cafe dan keduanya ingin mengakses internet menggunakan WiFi. Adi ingin menggunakan WiFi yang disediakan oleh cafe, sedangkan Bagas ingin menggunakan WiFi hotspot nya sendiri (e.g. modem 4G WiFi). Kebetulan, hotspot yang disetup Bagas menggunakan channel yang sama dengan access point WiFi milik cafe. Pada kasus ini, gawai Adi dan Bagas tidak akan dapat berasosiasi dan berkomunikasi dengan Access Point tujuan mereka masing-masing (asumsi mereka tidak transmit pada saat bersamaan).

Select one:

- ☐ True
- ☒ False ✓

Both of them can still associate to different access points although the access points operate in the same channel/frequency. They can also communicate with their respective access point, as long as they are not transmitting at the same time (concurrent transmission in the same channel leads to collision).

The correct answer is 'False'.

Question 7

Correct

Mark 1.00 out of 1.00

Sebuah WiFi host dengan protokol multiple access CSMA/CA akan segera menghentikan transmisi ketika host tersebut mendeteksi adanya packet collision.

Select one:

- ☐ True
- ☒ False ✓

Ability to detect collision and abort transmission when a collision is detected belongs to CSMA/CD

The correct answer is 'False'.

Question 8

Correct

Mark 1.00 out of 1.00

Radio Network Controller (RNC) pada jaringan 3G mengendalikan atau melayani beberapa BTS, dan juga memisahkan traffic voice dan traffic data.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Question 9

Correct

Mark 1.00 out of 1.00

Traffic voice dan traffic data dibuat terpisah pada jaringan LTE.

Select one:

- ☐ True
- ☒ False ✓

Voice traffic and data traffic are separated in 2.5G (GPRS) and 3G networks. But 4G LTE has unified architecture, i.e. all IP network architecture for all kinds of traffic (including voice and data)

The correct answer is 'False'.

Question 10

Correct

Mark 1.00 out of 1.00

Algoritma DES membutuhkan public key dan private key, sedangkan algoritma RSA hanya digunakan untuk enkripsi.

Select one:

- ☐ True
- ☒ False ✓

DES is symmetric key, so it has no public-private key pair. RSA can also be used to create digital signature

The correct answer is 'False'.

Question 11

Correct

Mark 1.00 out of 1.00

Proses enkripsi atau dekripsi menggunakan asymmetric cryptography lebih lambat daripada symmetric.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

Tentukan istilah/terminologi paling tepat pada setiap statement berikut:

Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message.

Confidentiality



Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi.

Authorization



Serangan yang dilakukan oleh banyak agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc).

Distributed Denial of Service



Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan.

Availability



Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan)

Integrity



Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target.

Spoofing



Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker.

Hijacking



Your answer is partially correct.

You have correctly selected 6.

The correct answer is: Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message. → Confidentiality, Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi. → Authentication, Serangan yang dilakukan oleh banyak agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc). → Distributed Denial of Service, Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan. → Availability, Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan) → Integrity, Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target. → Spoofing, Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker. → Hijacking

Question 13

Partially correct

Mark 2.00 out of 7.00

Cocokkanlah tujuan dari solusi cryptography berikut dengan notasi cryptography yang sesuai. Definisi dari notasi cryptography adalah sebagai berikut:

- m = message
- K_s = Symmetric key
- K_{s+} = Sender's public key
- K_{s-} = Sender's private key
- K_{r+} = Receiver's public key
- K_{r-} = Receiver's private key
- $H(m)$ = hashed of a message
- MAC = Message Authentication Code

Menjamin

kerahasiaan

sebuah message

Sender: $K_{r+}(m)$; Receiver: $K_{r-}(K_{r+}(m))$

menggunakan

public key

cryptography

Menjamin

integritas dan

authenticity

sebuah message

Choose...

menggunakan

symmetric key

cryptography

Menjamin

integritas dan

authenticity

sebuah message

Sender: $m, K_{s-}(H(m))$; Receiver: $H(m)$, verify($H(m) = K_{s+}(K_{s-}(H(m)))$)

dengan message

digest dan

public key

cryptography

Menjamin

kerahasiaan

sebuah message

menggunakan

kombinasi

Choose...

symmetric dan

public key

cryptography

Menjamin

integritas dan

authenticity

sebuah message

Choose...

menggunakan

public key

cryptography

Menjamin
kerahasiaan,
integritas dan
authenticity
sebuah message
menggunakan
kombinasi
symmetric dan
public key
cryptography

Choose...

Menjamin
kerahasiaan,
integritas dan
authenticity
sebuah message
menggunakan
message digest
serta kombinasi
symmetric dan
public key
cryptography

Choose...

Your answer is partially correct.

You have correctly selected 2.

The correct answer is: Menjamin kerahasiaan sebuah message menggunakan public key cryptography → Sender: $Kr+(m)$; Receiver: $Kr-(Kr+(m))$, Menjamin integritas dan authenticity sebuah message menggunakan symmetric key cryptography → $MAC(Ks, m)$, Menjamin integritas dan authenticity sebuah message dengan message digest dan public key cryptography → Sender: $m, Ks-(H(m))$; Receiver: $H(m)$, verify($H(m) = Ks+(Ks-(H(m)))$), Menjamin kerahasiaan sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: $Ks(m), Kr+(Ks)$; Receiver: $Kr-(Kr+(Ks)), Ks(Ks(m))$, Menjamin integritas dan authenticity sebuah message menggunakan public key cryptography → Sender: $m, Ks-(m)$; Receiver: verify($m = Ks+(Ks-(m))$), Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan kombinasi symmetric dan public key cryptography → Sender: $Ks(m, Ks-(m)), Kr+(Ks)$; Receiver: $Kr-(Kr+(Ks)), Ks(Ks(m, Ks-(m)))$, verify($m = Ks+(Ks-(m))$), Menjamin kerahasiaan, integritas dan authenticity sebuah message menggunakan message digest serta kombinasi symmetric dan public key cryptography → Sender: $Ks(m, Ks-(H(m))), Kr+(Ks)$; Receiver: $Kr-(Kr+(Ks)), Ks(Ks(m, Ks-(m))), H(m)$, verify($m = Ks+(Ks-(m))$)