Nama	
NPM	
Kelas	

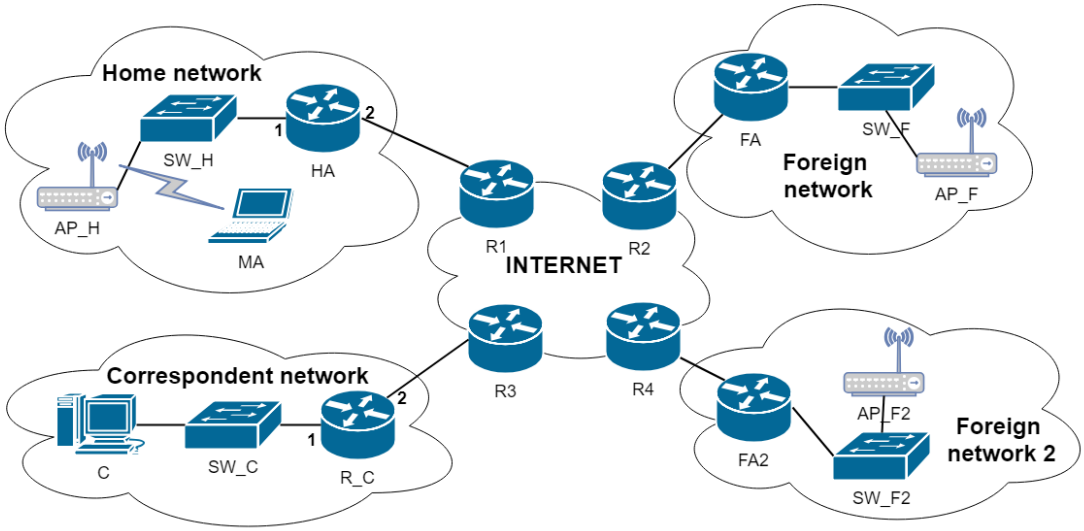
CSCM603154 – Jaringan Komputer
2018/2019 Term 1
Kuis # 4
12 Desember 2018
Waktu Kuis: 50 Menit

Beri tanda silang pada kolom B untuk pernyataan benar, atau pada kolom S untuk pernyataan salah dari pernyataan-pernyataan berikut! Total nilai: 20

B	S	Pernyataan
X		1. Jaringan wireless pada mode *ad-hoc* dapat menggunakan sebuah *controller* untuk melakukan routing packet antar node. *Jaringan wireless ad-hoc network seperti Bluetooth memiliki arsitektur master-slaves, di mana master mengatur kapan slaves dapat mengirim data.*
	X	2. Sebuah wireless terminal hanya menggunakan 1 teknik modulasi. Jika pada suatu saat SNR berkurang, maka BER juga semakin kecil. *Jika menggunakan modulasi yang sama, saat SNR berkurang maka BER akan semakin besar.*
X		3. Sebelum WiFi terminal mengirim frame, maka terminal tersebut akan melakukan sensing medium dahulu, dan frame tersebut akan dikirim jika medium dalam keadaan idle. *Cukup jelas → CSMA-CA*
	X	4. Pada jaringan LTE, traffic voice dipisahkan dengan traffic data. Sebelum LTE (2G dan 3G), traffic voice (conventional telephony) dipisah dengan data (IP based), tapi pada LTE hanya ada satu jenis traffic (IP based traffic).
	X	5. Pada proses *indirect routing* di jaringan GSM, awalnya panggilan diarahkan ke *Home Mobile Switching Center* (MSC) yang kemudian berkonsultasi dengan *Home Agent* (HA). *Indirect routing pada GSM, awalnya akan panggilan akan diarahkan ke home MSC, dimana home MSC ini akan berkonsultasi dengan **Home Location Register (HLR)**, lalu setelah itu panggilan akan diroute ke visiting MSC tempat mobile terminal yang dituju sekarang berada.*
	X	6. Algoritma **DES** memiliki kunci publik dan kunci privat, sedangkan algoritma **RSA** digunakan hanya untuk enkripsi. ***DES** adalah algoritma kunci simetris, sedangkan **RSA** adalah algoritma kunci publik/asimetris yang memiliki kunci privat dan publik.*
	X	7. Fungsi *hash* mengkonversi pesan dengan panjang tetap menjadi suatu nilai dengan panjang yang bervariasi. *Fungsi **hash** mengkonversi pesan yang panjangnya bervariasi menjadi suatu nilai dengan panjang yang fix.*
	X	8. Kantor pusat dan kantor cabang yang terhubung dengan IPSec akan memiliki 1 Security Association (SA). *Kantor pusat dan kantor cabang yang terhubung dengan IPSec akan memiliki 2 Security Association (SA), masing-masing untuk kantor pusat ke cabang dan sebaliknya.*

B	S	Pernyataan
X		9. 802.11i menggunakan *Authentication Server* (AS) yang terpisah dari *access point* untuk memperkuat security. *Cukup jelas*
X		10. *Stateful packet filtering firewall* dapat melakukan *tracking* terhadap semua koneksi TCP. *Cukup jelas*

Jawablah pertanyaan dari setiap soal berikut!
Gunakan gambar berikut untuk mengerjakan soal 1 dan 2!



1. (12 points) [**MAC dan IP Address**] Sebuah *Correspondent* (**C**) yang berada pada *Correspondent Network* mengirim paket kepada *Mobile Agent* (**MA**) yang berada pada *Home Network*. Tentukan *Source* serta *Destination* **MAC Address** dan **IP Address** dari paket yang dikirimkan dengan melengkapi tabel di bawah, dengan format sebagai berikut: **MAC-Perangkat** dan **IP-Perangkat**, atau **MAC-Perangkat-NoInterface** dan **IP-Perangkat-NoInterface**. **Contoh penulisan**: MAC-C, IP-MA, MAC-R_C-1, IP-HA-2. **Catatan:** Router **R_C** dan **HA** memiliki nomor interface 1 dan 2 seperti tertera pada gambar, dan TIDAK ada **NAT**.

Lokasi	IP Source	IP Destination	MAC Source	MAC Destination
C → R_C	IP_C	IP_MA	MAC_C	MAC_R_C-1
HA → AP_H	IP_C	IP_MA	MAC_HA-1	MAC_MA

Lokasi	Address 1 (Receiver)	Address 2 (Sender)	Address 3 (Router)	Address 4 (Utk ad-hoc)
AP_H → MA	MAC_MA	MAC_AP_H	MAC_HA-1	

2. [**Mobile IP**] Anggap IP address **C**: 123.1.2.3, IP address **MA** (*Permanent Address*): 70.70.70.70, IP address **HA**: 70.70.70.1, Care of Address (CoA) **FN**: 200.1.1.1, dan CoA **FN2**: 180.1.1.1.
   (a) (8 points) Saat ini **C** dan **MA** sedang melakukan sesi *video streaming*, di mana saat ini **MA** sedang berada di **Foreign Network** (**FN**). Lengkapi tabel di bawah untuk menggambarkan proses *indirect routing* antara **C** dan **MA**! **Note**: Kolom payload/isi hanya untuk paket yang memiliki kandungan payload/isi yang relevan saja.

Pengirim	Penerima	Dest. IP Address	Payload/isi
C	HA	70.70.70.70	
HA	FA	200.1.1.1	paket no 1 (pada proses yang sebelumnya)
FA	MA	70.70.70.70	
MA	C	123.1.2.3	

(b) (10 points) Saat sesi tengah berlangsung, **MA** berpindah ke **Foreign Network 2** (**FN2**) sambil tetap menjaga konektifitas dengan **C** dengan protokol *Mobile IP* menggunakan metode *Indirect Routing*. Tuliskan proses *discovery* dan registrasi saat **MA** pindah ke **Foreign Network 2** dengan melengkapi tabel di bawah ini!

Pengirim	Penerima	Dest. IP Address	Jenis message
FA2	MA	70.70.70.70	ICMP agent advertisement
MA	FA2	180.1.1.1	registration request
FA2	HA	70.70.70.1	registration request
HA	FA2	180.1.1.1	registration reply
FA2	MA	70.70.70.70	registration reply

(c) (8 points) Tuliskan proses proses *indirect routing* antara **C** dan **MA** setelah **MA** pindah ke **Foreign Network 2** dengan melengkapi tabel di bawah ini! **Note**: Kolom payload/isi hanya untuk paket yang memiliki kandungan payload/isi yang relevan saja.

Pengirim	Penerima	Dest. IP Address	Payload/isi
C	HA	70.70.70.70	
HA	FA2	180.1.1.1	paket no 1 (pada proses yang sebelumnya)
FA2	MA	70.70.70.70	
MA	C	123.1.2.3	

3. Alice (**A**) ingin mengirim pesan **m** ke Bob (**B**).

(a) (2 points) Jika pesan **m** yang dikirim dienkripsi menggunakan *symmetric key cryptography* untuk menjamin kerahasiaannya, dimana K_S = symmetric key, $K(m)$ = enkripsi pesan **m** dengan kunci **K**, dan $K'(K(m))$ = dekripsi cipher-text dengan kunci **K'** untuk mendapatkan kembali **m**. Tuliskan proses enkripsi yang dilakukan **A** dan dekripsi yang dilakukan **B** menggunakan notasi tersebut!

Solution: Enkripsi oleh **A**: $ciphertext(c) = K_S(m)$
Dekripsi oleh **B**: $m = K_S(K_S(m))$

(b) (4 points) Jika pesan **m** yang dikirim dienkripsi menggunakan *public key cryptography* untuk menjamin kerahasiaannya, di mana K_A^+ = public key **A**, K_A^- = private key **A**, K_B^+ = public key **B**, K_B^- = private key **B**, $K(m)$ = enkripsi pesan **m** dengan kunci **K**, dan $K'(K(m))$ = dekripsi cipher-text dengan kunci **K'** untuk mendapatkan kembali **m**. Tuliskan proses enkripsi yang dilakukan **A** dan dekripsi yang dilakukan **B** menggunakan notasi tersebut!

Solution: Enkripsi oleh **A**: $ciphertext(c) = K_B^+(m)$
Dekripsi oleh **B**: $m = K_B^-(K_B^+(m))$

(c) (10 points) Jika pesan **m** yang dikirim dienkripsi menggunakan kombinasi *symmetric key* dan *public key cryptography* untuk menjamin kerahasiaan pesan dan kunci simetrik, dengan notasi yang sama seperti pada poin (a) dan (b). Tuliskan semua proses yang dilakukan serta apa saja yang dikirim oleh **A**, dan proses yang dilakukan **B** setelah menerima apa saja yang dikirim **A**!

Solution: Pesan dienkripsi dengan symmetric key oleh **A**: $K_S(m)$
Lalu symmetric key dienkripsi dengan public key **B**: $K_B^+(K_S)$
Lalu **A** mengirim $K_S(m)$ dan $K_B^+(K_S)$ ke **B**
B mendapatkan K_S menggunakan K_B^-: $K_B^-(K_B^+(K_S))$
Lalu **B** mendapatkan m menggunakan K_S yang didapatkan sebelumnya: $m = K_S(K_S(m))$

(d) (6 points) Jika pesan **m** yang dikirim ditambahkan *digital signature* untuk menjamin integritasnya, dengan notasi yang sama seperti pada poin (b), dengan pengecualian: $K(m) =$ pembuatan digital signature dari pesan **m** dengan kunci **K**, dan $K'(K(m)) =$ validasi digital signature dari pesan **m** dengan kunci **K'**. Tuliskan semua proses yang dilakukan serta apa saja yang dikirim oleh **A**, dan proses yang dilakukan **B** setelah menerima apa saja yang dikirim **A**!

Solution: Digital signature oleh **A**: $d = K_A^-(m)$
Lalu **A** mengirim $d = K_A^-(m)$ dan m ke **B**
B memvalidasi d: $K_A^+(K_A^-(m))$ dengan m yang dikirim bersamaan

(e) (10 points) Jika pesan **m** yang dikirim ditambahkan *digital signature* dengan fungsi *hash* untuk menjamin integritasnya dengan notasi yang sama seperti pada poin (d), ditambah $H(m) =$ hasil *hash* dari pesan **m**. Tuliskan semua proses yang dilakukan serta apa saja yang dikirim oleh **A**, dan proses yang dilakukan **B** setelah menerima apa saja yang dikirim **A**!

Solution: Digital signature oleh **A**: $d = K_A^-(H(m))$
Lalu **A** mengirim $d = K_A^-(H(m))$ dan m ke **B**
B menghitung hash dari $m \rightarrow H(m)$
Lalu **B** memvalidasi d: $K_A^+(K_A^-(H(m)))$ dengan $H(m)$ yang sudah dihitung sebelumnya

4. (12 points) Tuliskan/jelaskan proses (*real*) *handshake* pada **SSL**!

Solution:

1. Client mengirimkan list algoritma yang disupport + nonce client (R_C) ke server

2. Server memilih salah satu algoritma (choice) dari list yang diberikan client; lalu mengirimkan: choice + sertifikat server ($cert_{server}$) + nonce server (R_S)
3. Client memverifikasi $cert_{server}$ dan mengekstrak K_S^+ dari $cert_{server}$; mengenerate pre_master_secret lalu di-enkripsi dengan public key server ($K_S^+(pre\_master\_secret)$) dan dikirim ke server
4. Client dan server menghitung kunci enkripsi (K) dan kunci MAC (M) secara independen, dari pre_master_secret, R_C dan R_S
5. Client mengirim MAC dari semua pesan handshake yang dikirim nya
6. Server mengirim MAC dari semua pesan handshake yang dikirim nya