Part I. Wireless Networks Security Facts (50%)

This part consists of 25 multiple choice questions. The assessment weight is equally distributed over all the questions in this part. Each question gives four possible answers, but only one is correct. Marking the correct answer results in 2 points, whereas double, wrong or missing mark result in zero. *Please use the attached sheet for marking your answers to this Part I.*

1. Is the same key used for both authentication and encryption in WEP?

   a) Yes
   b) No
   c) Yes, if 802.1X authentication is not used
   d) The same key is never used twice

2. How does WEP detect replay?

   a) There is no replay detection
   b) By the intialization vector (IV)
   c) By the integrity check value (ICV)
   d) By the random nonce value (RNV)

3. How long is the IV used in TKIP?

   a) 24 bits
   b) 48 bits
   c) 64 bits
   d) 128 bits

4. Which protocol encapsulates the EAP messages transported between the supplicant and authenticator in WPA/RSN?

   a) EAP-TLS
   b) EAPOL
   c) 802.11
   d) 802.1X

5. What is the purpose of the first phase of PEAP?

   a) The supplicant provides the identity to the authentication server
   b) The supplicant and authentication server negotiate the EAP method to be used
   c) The supplicant encrypt and communicate the password to the authenticator
   d) Supplicant establishes an authenticated secrecy channel to the authentication server

6. Which 802.11 frame type is cryptographically protected by the 802.11w standard?

   a) Management frames
   b) Control frames
   c) Data frames
   d) Beacon frames

7. How is the 128 bits start value of the counter for CCMP encryption initialized in RSN?
   - a) By a random IV
   - b) By the concatenation of IV and the extended IV
   - c) By the concatenation of flag/priority bits, packetnumber, source-address, and a constant
   - d) By source address, destination address and the MIC value of the MPDU
8. What is the key size of AES as used in RSN?
   - a) 128 bits
   - b) 192 bits
   - c) 256 bits
   - d) 512 bits
9. Does EAP-SIM provide mutual authentication?
   - a) No, it uses the regular GSM authentication
   - b) Yes, it uses the regular UMTS authentication
   - c) Yes, by the regular GSM authentication and the authentication token from the AuC
   - d) Yes, by the regular GSM authentication and a nonce in the encrypted AP response
10. What is the purpose of the EAPOL 4-way handshake?
    - a) To exchange a fresh pairwise temporal key (PTK) from the pairwise master key (PMK)
    - b) To exchange a fresh pairwise message key (PMK) from the pairwise transient key (PTK)
    - c) To exchange a fresh pairwise transient key (PTK) from the pairwise master key (PMK) with bilateral key agreement and group key transfer
    - d) To exchange a fresh pairwise message key (PMK) from the pairwise trusted key (PTK) generated in the 4-way key agreement including group key distribution
11. What are the four types of EAPOL messages used in WPA/RSN?
    - a) Start, Key, Packet, Logoff
    - b) Request, Authenticate, Result, Stop
    - c) Identity, Challenge, Response, Accept
    - d) Logon, Name, Password, Logoff
12. What is the purpose of the sequence number (SQN) used in 3G/UMTS networks?
    - a) The USIM can detect replay of authentication messages
    - b) The VLR/SGSN can detect replay of authentication messages
    - c) The UE can verify the MAC values by using $f1$
    - d) The HLR/AuC can generate distinct session keys
13. List the message authentication code types used in UMTS
    - a) MIC, MAC
    - b) MAC-A, MAC-I, MAC-S

c) IK, AK
d) AUTN, AUTS

14. What are the three most important security services in GSM?

a) User authentication, radio channel confidentiality, and temporary identities
b) Subscriber Identity Module, Visiting Location Register, and Authentication Centre
c) User identification, end-to-end encryption, and symmetric key exchange
d) The cryptographic algorithms A3, A5 and A8

15. What are the variables of the authentication token (AUTN) used in UMTS networks?

a) $SQN \oplus AK$, XRES, MAC
b) $SQN \oplus AK$, AMF, MAC
c) SQN, AMF, MAC, RAND
d) $SQN \oplus AK$, AMF, MAC, RAND

16. Which UTRAN layers provide encryption?

a) MAC layer and RRC layer
b) RLC layer and RRC layer
c) PHY layer and MAC layer
d) MAC layer and RLC layer

17. Which UTRAN layer provides integrity protection?

a) MAC layer
b) RLC layer
c) RRC layer
d) PHY layer

18. What is a call session control function (CSCF)?

a) A SIP server or proxy used in IMS
b) A Mobile Switching Centre (MSC) with IMS support
c) A GPRS Support Node (GSN) with IMS support
d) A Real-time Transport Protocol (RTP) session controller used in IMS

19. What is the length of the cipher key CK used in UMTS?

a) 56 bits
b) 64 bits
c) 128 bits
d) 256 bits

20. How many rounds does the KASUMI cipher use?

a) 8

b) 10

c) 12

d) 16

21. What kind of cipher is KASUMI?

 a) Stream cipher

 b) Feistel cipher

 c) Substitution-permutation cipher

 d) Nonlinear feedback shiftregister cipher

22. Why is the UICC normally easily removable from the mobile station?

 a) The USIM holds an expiration date and, like credit cards, must be replaced

 b) The failure rate of the integrated circuit cards (UICCs) are high because the issuers (mobile operators) want to optimize cost against subscription duration

 c) End-to-end UMTS key-card plugs into the USIM slot for key distribution and management

 d) The UE manufacturing and lifecycle can be managed independently from the personalization and subscription process

23. Why must the USIM implementation be tamper-proof?

 a) To facilitate the mobile operator with secure computation and storage at the UE side

 b) To protect the proprietary crypto-algorithms of the mobile operator

 c) To protect the subscriber against unauthorized modification of the subscription parameters

 d) To provide the subscriber with a PIN-protected access to the UMTS service

24. How is a oneway hash function useful in digital forensic investigations?

 a) For fast recognition of known file content

 b) For reconstructing the hash tables of deleted files

 c) For juridical determination of incriminating file content

 d) For legally sound presentation of the digital evidence

25. What are the purpose of the MILENAGE functions in UMTS?

 a) Block cipher family of functions that build the algorithms for integrity code and the encryption process

 b) Transformation of keys for the inter-operation of GSM and UMTS basestations and networks

 c) Pseudorandom generators that output the initializing values for the cryptographic computations

 d) Algorithms for computing the cryptographic variables needed in the mutual authentication protocols

Part II. Authentication Protocols (35%)

As head of the communication security team in Telematics Inc. you are responsible for the design of the authentication protocol between mobile equipment UE and a new radio access network VTRAN being developed. You and your team start thinking about the problem by recapitulating the UMTS Authentication and Key Agreement protocol, denoted $\mathcal{U}$ here. Soon you have constructed a new and promising protocol proposal $\mathcal{V}$ to be analyzed. You want to use the same cryptographic functions as in UMTS. Here is $\mathcal{V}$:

UE		VTRAN
Memory (IMSI, SID, K)		**Database** $\{$(IMSI, XSID, K)$\}$
RAND $\leftarrow f0()$		
SID $\leftarrow$ SID $+ 1$		
MAC $\leftarrow f1_K$(IMSI, RAND, SID)		
AUTV = (IMSI, RAND, MAC)		
	$\xrightarrow{AUTV}$	
		Select XSID, K **of received** IMSI
		Verify1
		RES $\leftarrow f2_K$(RAND)
	$\xleftarrow{RES}$	
Verify2		
Store SID	$\xrightarrow{ACK}$	**Store** XSID $\leftarrow$ XSID $+ 1$

Here in $\mathcal{V}$, the SID, XSID (session identifier) and MAC values are 64 bits each, ACK is 1 bit, and the rest of the parameters are each 128 bits.

26. Specify the procedure of the **Verify1** step on the VTRAN side, and the procedure of the **Verify2** step on the UE side. (10%)

27. Which new functions, compared to $\mathcal{U}$, do you find must be implemented for $\mathcal{V}$? Propose how these functions can be implemented.(5%)

28. Calculate the number of bits in the message exchange of $\mathcal{V}$, and compare this to $\mathcal{U}$.(5%)

29. Now refine the structure of the VTRAN into the Radio Access part (BST/RNC), the Visited Network, and the Home Network. Specify how you will enhance the protocol $\mathcal{V}$ to provide encryption and integrity keys that can be used to set up a secure channel between UE and RNC. (5%)

30. You foresee that the SID and XSID values will not remain properly synchronized under all error conditions. Specify how you will solve this problem of re-synchronization. (10%)

Part III. WEP Cryptanalysis (15%)

Shannon proposed to measure the amount of information using the concept of entropy. Here we will use the word *uncertainty*. Let $x_0, ..., x_{n-1}$ be n the possible values for a random variable X. Let $p_i = \Pr[X = x_i]$, for instance p_{42} is the probability that $X = x_{42}$. The uncertainty associated with the random variable X is defined as

$$H(X) = -\sum_{i=0}^{n-1} p_i \log_2 p_i \ .$$

The uncertainty is measured in bits, is a real number and can be smaller than 1. If the variable X is transmitted using $R(X)$ bits then the *redundancy* of this coding is defined as

$$D(X) = R(X) - H(X) \ .$$

Informally, $D(X)$ is the amount of wasted bits used to transmit X, because in theory X can be transmitted with $H(X)$ bits using the best possible lossless compression.

In cryptanalysis, the redundancy of the ciphertext, as a random variable X, may be used to extract the information about the secret key K. The *unicity distance* is the number of observations of X needed to uniquely determine K. It is defined as

$$U = \frac{H(K)}{D(X)} \ .$$

The formula can be roughly understood as follows. Every new observation of X leaks $D(X)$ bits of information about the key K, and thus decreases our original uncertainty $H(K)$ by $D(X)$ bits.

In WEP, the packet key is constructed as IV||Rk. Klein has derived a probabilistic relation between the first byte Rk[0] of the root key and the values of IV and the keystream byte Ks[2]:

$$\Pr\left[\underbrace{\mathrm{Rk}[0]}_{k} = \underbrace{S_3^{-1}[\,3 - \mathrm{Ks}[2]\,] - (S_3[3] + j_3)}_{X}\right] \approx \frac{1.36}{256} \ ,$$

where S_3 and j_3 are internal variables of RC4 that can be computed from the IV. With the introduced notation for the key byte k and the variable X we can write

$$p_k = \Pr[\,X = k\,] \approx \frac{1.36}{256} \ . \tag{1}$$

We also assume that the variable X takes on all of the other 255 values with equal probability

$$p_i = \Pr[\,X = i\,] = \frac{1 - p_k}{255}, \ \text{for all } i \neq k \ . \tag{2}$$

31. When a byte variable X is assigned a random value, in other words sampled from the uniform probability distribution over $\{0, 1, ..., 255\}$, what is the probability that X takes on the value 42? Calculate the uncertainty $H(X)$.(3%)

32. Now we skew the probability distribution of X slightly. For some fixed value k, the probability that X takes the value k is given in Eq. 1 and the probability for each of the other values is given by Eq. 2. Calculate the uncertainty $H(X)$ for this probability distribution.(3%)

33. The byte variable X defined in Question 32 is transmitted using 8 bits. Calculate the redundancy $D(X)$.(3%)

34. An attacker sniffs ARP packets (known plaintext) transmitted in a wireless network that is secured by WEP. Calculate the number of observations of *distinct* IVs needed to recover uniquely the first byte Rk[0] of the network root key.(3%)

35. From the generalized birthday problem we know that when n values are randomly selected, with replacement, from a domain of m values, the expected number of *distinct* values observed is

$$E(m,n) = m\left(1 - \left(1 - \frac{1}{m}\right)^n\right) \quad .$$

Let us apply this to WEP packet sniffing where the IV values are chosen at random. Then m represents the total number of possible IV values, and n represents the number of ARP packets captured, hence $E(m,n)$ represents the expected number of *distinct* IV values observed. Calculate the total number of ARP packets that should be captured such that the expected number of distinct IVs equals the number obtained in Question 34.(3%)