1. List security objectives and briefly describe their goals

   - Authentication
   - Data integrity
   - Data confidentiality
   - Misbehavior detection and revocation

2. Enumerate the main security adversaries

   - Individuals operating on their own with limited resources: Computer hackers or electronics hobbyists
   - Loosely coordinated groups with more resource than each individual: Sharing private keys with collaborators to collectively multiply the damages
   - Insiders owning sensitive information about security protection system for an organization
   - Adversary organizations with abundant resources and sophisticated technologies
   - Foreign governments interested in mounting security attacks to nation's vehicle networks
   - Government agencies permitted to breach driver privacy

3. List four security threats and briefly explain their objectives

   - Send false safety messages using valid security credentials
   - Falsely accuse innocent vehicles
   - Impersonate vehicles or network entities
   - Denial-of service attacks

4. Give three classes of security techniques for basic security algorithms

   - Cryptographic algorithms: Mathematical transformation of input data (data and keys) to output data. It is used in cryptographic protocols
   - Cryptographic protocols: Series of steps and message exchange between multiples entities to achieve a specific security objective
   - Security-supporting mechanisms: Provide security-relevant functionalities as a part of a cryptographic protocol

5. How does the encryption of data work?

   - Encryption of data is the transformation of plaintext data into ciphertext in order to conceal its meaning. Cryptographic encryption algorithm is used in combination with a key

6. Provide a comparison between symmetric and asymmetric encryption

   - Symmetric encryption: Single shared key is used for encryption and decryption, eg. two nodes (sender and receiver) have to be in possession with the same key but not other entity
   - Asymmetric encryption: Two different keys for encryption and decryption. Public key of the receiving node is used to encrypt the data whereas the sender uses it own private key to decrypt the data

7. How does the process of signing of data work?

   - Signing of data is referred to the computation of a check value or an assignment of a digital signature to a given plain text or ciphertext
   - Process is depicted on lecture slide 19

8. What is the role of Certificate Authority (CA)?

   - CA secures the certificate itself by signing it with his private key. Public key of the CA must be known in advance to receivers of a signed message

9. Provide a description of the X.509 certificate and its content

   - See lecture slide 21

10. What is the role of the Public Key Infrastructure (PKI)?

    - PKI distributes digital certificates to all participating communication entities needed for the authentication of valid participants

11. Provide an overview of the PKI architecture

    - See lecture slide 24

12. What is the role of following authority: root certificate authority, long term certificate authority, and pseudonym certificate authority?

    - RCA defines common policies among all subordinate LTCAs and PCAs
    - LTCA issues long-term certificates (LTCs) to ITS stations
    - PCA issues pseudonym certificates (PCs) to ITS stations

13. Briefly provide the main benefits of PKI

    - See lecture 28-29

14. List some aspects of privacy

    - Privacy of location

- Privacy of interests
- Privacy of social standing
- Privacy of social network

15. Why does security limit the level of privacy?

    - Security measures reduce the level of privacy because identities are strongly bound to the vehicles
    - Although each CAMs is secured using a digital signature, the vehicle still reveals its identity through the certificate used

16. How to prevent location tracking of a vehicle from third parties?

    - Through pseudonymity as pseudonym prevents identification/re-identification when using a certain number of different identities instead of using a single identity

17. How does the generation of pseudonyms work?

    - See lecture slide 35

18. List some switching strategies of pseudonyms

    - Fully random
    - Periodic: switch to another pseudonym every n seconds
    - Geographical: switch to another pseudonym depending on region/area
    - Vehicle dynamics and communication quality: Use of position, speed, heading and number of cars in transmission range to trigger a pseudonym change

19. What is the main security challenge for the V2X system?

    - Computational overhead: For each CAM sent and received, complex asymmetric cryptographic algorithms need to be executed