1. The three types of sciences: inductive, deductive, and reductive. An overview of the scientific method.

Understand the differences between inductive (from observation to generalization), deductive (from axioms to conclusions), and reductive (breaking down complex phenomena). Be able to outline the general steps of the scientific method.

2. The hierarchical levels of information, the concepts of sets and systems, the multi-level model of informational properties, and the concept of a signal and its basic types.

Know how information can be described on multiple levels (statistical, syntactic, semantic, etc.). Be able to define sets, systems, and basic signal types with examples.

3. The quantitative properties of information, the concept of relative frequency, probabilities in finite event systems, Shannon's information-measuring function, the statistical properties of message sets, and the entropy and redundancy of a message set.

Be able to calculate probabilities, apply Shannon’s formula, and explain what entropy and redundancy mean in the context of messages.

4. The syntactic properties of information. The concept of a code. Properties of different code types. Encoding messages, the Shannon-Fano procedure.

Understand what a code is, why coding is necessary, and the key properties of various code types. Be able to illustrate the Shannon–Fano coding procedure with a simple example.

5. The concept of parity bit, Hamming distance, and correcting a 1-bit error in 16-bit data.

Understand how parity bits detect errors, what Hamming distance means, and how a single-bit error can be corrected in a given data word.

6. Other error detection and correction methods: the concept of a checksum. Elias block protection.

Understand the principle of checksums and how Elias block protection enhances reliability.

7. Checksum. The protection algorithm of bank card numbers and tax numbers.

Understand how checksums are applied in practice, e.g., the Luhn algorithm for bank cards and checksum rules in identifiers.

8. Simple compression methods: RLE coding, LZW coding.

Be able to explain how RLE compresses repeated data and how LZW is used for general-purpose compression.

9. Character codes: ASCII codes, Unicode, UTF-8 encoding and decoding.

Understand the differences between ASCII and Unicode and why UTF-8 is necessary for representing multilingual texts.

10. Demonstration of Base64 encoding and decoding.

Explain how Base64 converts binary data into text and give examples of its use (e.g., email attachments, data in JSON).

11. Demonstration of JPEG and MPEG compression, including their key properties.

Know the basics of lossy compression, including why JPEG is used for images and MPEG for video.

12. The syntax of languages: demonstration of Backus-Naur (BN) form, syntax graphs, JSON schema, the essence of XML and DTD, YAML syntax.

Be able to describe formal syntax notations (BNF, syntax graphs), understand JSON schemas, and explain the purpose of XML and DTDs, JSON and YAML.

13. Implementation of key exchange protocol over an insecure (eavesdropped) channel.

Understand the principle of the Diffie–Hellman key exchange and why it works securely even if the channel is monitored.

14. The essence of RSA encryption.

Explain how RSA works using prime numbers, public and private keys, and why it is secure.

15. Hash codes and their properties, password storage.

Know the main properties of cryptographic hash functions (collision resistance, etc.) and how hashes with salt are used for secure password storage.

16. Digital signatures with and without hash codes.

Understand how digital signatures work, and why using hash functions makes them more efficient and secure.

17. Public key authentication, with a CA.

From:
https://edu.iit.uni-miskolc.hu/ - **Institute of Information Science - University of Miskolc**

Permanent link:
https://edu.iit.uni-miskolc.hu/tanszek:oktatas:techcomm:examination_questions

Last update: **2025/12/12 10:01**