TK2100

# T-01

KRYPTERING

1. Hva er kryptering
   * The art of withing and solving codes
2. Hva er substitusjonschiffer
   * a **substitution** cipher is a method of encrypting in which units of plaintext are replaced with the ciphertext in a defined manner
3. Kan man bruke subsitusjon på binærtall?
   * Ja
4. Hva er «One-Time pads» og er dette sikkert?
   * The one-time pad is an encryption technique that cannot be cracked but requires a single-use pre-shared key that is no smaller than the message being sent.
   * The key cannot be used more than once.
5. Hva står «AES» for?
   * Advanced Encryption Standard
6. Hvilke av disse er «AES» versjoner?
   * AES-128
   * AES-192
   * AES-256
7. Er «AES» 100% sikkert? Yes, AES-256 is currently unbreakable. The only quantum machine that can break the code is a quantum machine that attains level 2064. The current level is 64.
8. Hva er asymetrisk kryptering (public key kryptering)
   * Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys. Each pair consists of a public key and a private key. The generation of such key pairs depends on cryptographic algorithms, which are based on mathematical problems termed one-way functions.
9. Hva er Symetrisk kryptering?
   * Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext. The keys may be identical, or there may be a simple transformation to go between the two keys.
10. Er «RSA» Symetrisk eller asymetrisk?
    * Asymetrisk
    * RSA is named for the MIT scientists (Rivest, Shamir, and Adleman) who first described it in 1977. It is an **asymmetric algorithm** that uses a publicly known key for encryption, but requires a different key, known only to the intended recipient, for decryption.
11. Er «AES» Symetrisk eller asymetrisk?
    * Symetrisk

Is AES encryption symmetric or asymmetric? AES is **a symmetric encryption algorithm** because it uses one key to encrypt and decrypt information, whereas its counterpart, asymmetric encryption, uses a public key and a private key.

1. Forklar hvordan en person ville startet en samtale med «RSA», men senere byttet til «AES» like etter. Hvorfor ikke bruke «AES» hele tiden? Eller hvorfor ikke bare bruke «RSA»?

Yes, one can use the security attained by RSA combined with the performance of the AES algorithm. If Alice and Bob do not know of each other’s private key they can initiate secure communication by use of RSA (separate private keys/ one public key), exchange a common private key securely, and continue the communication over AES using the private key.

1. Hva er en kryptografisk nøkkel?
   * A key in cryptography is a piece of information, usually a string of numbers or letters

that are stored in a file, which, when processed through a cryptographic algorithm, can encode

or decode cryptographic data.

1. Forklar hva SHA-256 er?
   * **SHA 256** is a part of the SHA 2 family of algorithms, where SHA stands for Secure

Hash Algorithm.