1 Crypto intro and historical

1. While most use CIA as the foundation for Information Security some add further words to complete it. Name two more commonly used to enhance the triad (CIA triad: confidentiality, integrity, availability)
   - Answer: Authenticity, Accountability, Non-repudiation (no one can deny the validity, e.g. transaction has taken place)
2. Cryptography is usually used to achieve or provide a so-called cryptographic service. Name methods or functions (aka cryptographic primitives to achieve the listed services).
   - Data secrecy: encryption
   - Data integrity: digital signatures (signed hashes)
   - User verification: Authentication: via private/public key cryptography (e.g. certificates), hash fucntions and random number (e.g. challenge response pw authentication)
   - Non-repudiation: private key cryptography
3. We usually refer to Alice and Bob as parties that exchange information. Could you name three more personas that have a special meaning in crypto? Eg. Mallory for someone that does malicious thing
   - Oscar: an opponent (similar to Mallory but not necessarily malicious)
   - Dan (my favorite): generic paticipant
   - Eve: an eavesdropper.. tries to read messages but won't (can't) modify messages
4. raw a basic crypto system and name all inputs, outputs, intermediate products, processes as well as all involved parties above. Diagram for the (very) poor showing symetric encryption:
   Attacker cannot read message (without key)
   Alice > encrypt message with key A > ~~~~~~~~ encrypted msg is sent ~~~~~~~~~~~~ > decrypt message with key A > Bob ready msg
5. Assuming Malory has no access to Alice and Bobs facilities but is in position to interfere with and to snoop on the messages they exchange. Can you point out the difference between active and passive attacks which Mallory could apply? Give examples for both.
   - Active attack: modify message, replay, etc. (basically anything that modies the data stream)
   - Passive attack: listening (and decrypting) messages. Does not change data being sent.
6. Alice and Bob could make use of two major concepts to secure their messages. Either use a symmetric cipher systems or a public key cipher systems. Explain the difference based on Wikipedia, Cryptography, Modern Cryptography, Sections Symmetric and Public-key encryption
   - Symmetric ciphers use the same key to encrypt and decrpyt data. Sender and receiver therefore both need access to the same key.
   - Public key (or asymetric) ciphers require a different keys for encryption and decryption. Usually, one key is kept secrect - the private key - and and the other is public. Public key cryptography is not only used to provide data secrecy but is also a fundamental building block for other aspects of cryptography such as data integrity, authentication.
7. Genius engineers such as Alice are capable to developed their own algorithms to secure messages. Is it a wise decision to keep the algorithms secret? Discuss pros and cons.
   - It is not wise as a non published algorithm is not really put to the test. The inner workings of the algorithm might be leaked to the public and the system operates with a non-tested algorithm.
8. (optional) -> I failed with online tools (but didnt search long as it is optional). A simple substitutaion cipher should be relativly easy to decipher by statistics (most common letters, very commen words etc.)
9. (optional) -> I assume it probably the mary stuart cipher, which seems slightly more complicated to decipher it is not like each letter corresponds to a letter in the decoded text (some words map to one

letter, some letters have no corresponding encryption letter etc.)

10. Is a cipher text properly protected if we make sure to have large keys? May you provide an example with the simple substitution cipher? - Example: (very) simple Substitution:
    - plaintext: "World"
    - Cypertext alphabet (only used letters): ABCDLORW -> ZYXWQMTS
        - Remark: just scrambled the letters a bit ..
    - Encryption: "SMTQW"

```
- From my understanding, a text encrypted with some subustituation ciphers can be
hard to break when the key is large:
    - Nomenclator: according to wikipedia, some historical encryptions have not
been cracked yet. I assume making the tables bigger (substitute more words
basically) makes the cipher harder to analyize.
    - I assume that substitution ciphers with a key so large that letters are
never represented by the same symbol in a given text cannot be decrypted probided
the attacker has no clue about the contect of the text. Frequency analysis would
be impossible. (homophonic substitution ciphers or polalphabetic substitution
could have this characteristic)
11. If Alice and Bob had choosen to hide the message with a One-Time Pad. Could we
decipher it? Name three things they needed to keep attention on to have perfect
secrecy and thus to avoid an attacker could recover the plain-text?
    - 1. key must be random
    - 2. key must be as long as the plaintext
    - 3. key msut only be used once
    - 4. key must only known by sender and receiver
```