Summary for task x

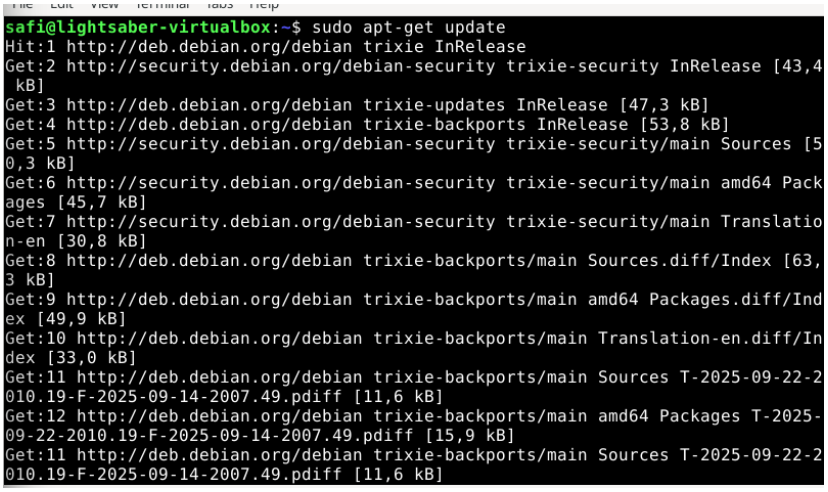
Applied cryptography Chapter 1:

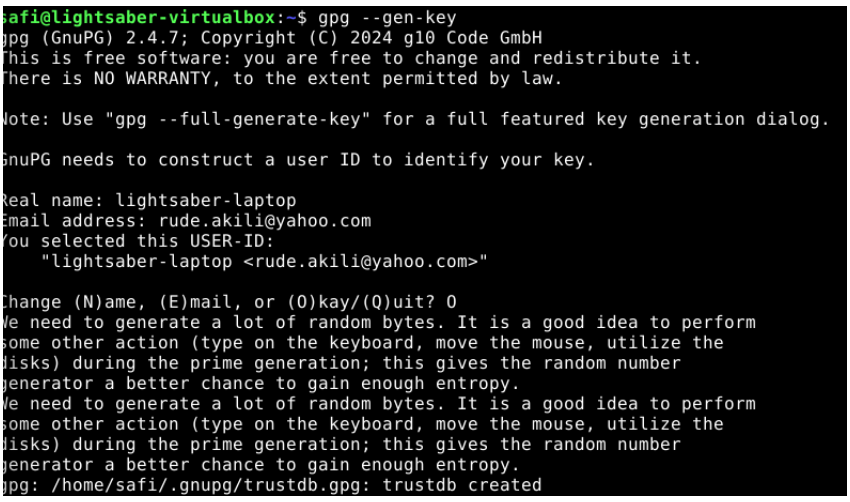
- encrypting (E) means to hide a **message (M)**; plaintext (P) or cleartext, turning it into cyphertext (C)
    - It is any kind of binary data such as a stream of bit, text file, a stream of digitalized voice, image, video etc.
- decryption (D) is a process of turning cyphertext into the message
- cryptography: keeping messages secure
- letters create functions on how encryption flows to decryption
    - Encrypting: E(M)=C
    - Decrypting: D(C)=M
    - The full function of encrypting and then decrypting: D(E(M)) =M
- In cryptography there are three vital components: authentication, integrity, nonrepudiation
    - authentication: there must be a possibility to verify as the receiver of the message
    - integrity: it can be proved by the receiver that the message has not been altered during transit
    - nonrepudiation: sender can’t deny sending a message
- steganography: hides secret messages in another message
    - this can be in an image
- substitution cipher: characters are substituted by a different character
    - homophonic: plaintext characters can be several characters at the same time
    - polygram: blocks of characters encrypted in groups
    - polyalphabetic: many substitutions cipher used together to encrypt
        - Caesar cipher: characters replaced with the third character
- transposition cipher: order of characters has been changed
    - plaintext is written horizontally for example (simple columnar)
- rotor machines: created to automate encryption
- perfect encryption scheme is one-time pad
    - a large nonrepeating random set of key letters on paper glued together

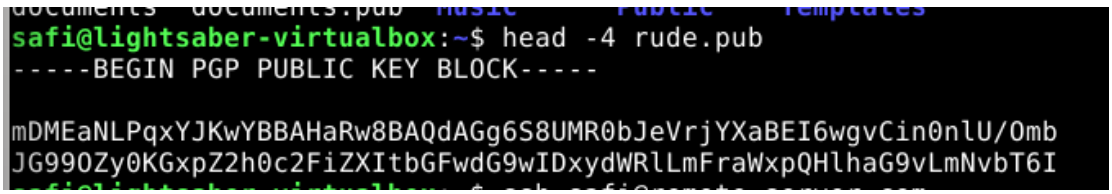
- Most popular computer encryption algorithms DES
    - symmetric algorithm, same key used for encryption and decryption.
- RSA: popular public-key algorithm
- DSA: can't be used for encryption, just digital signatures

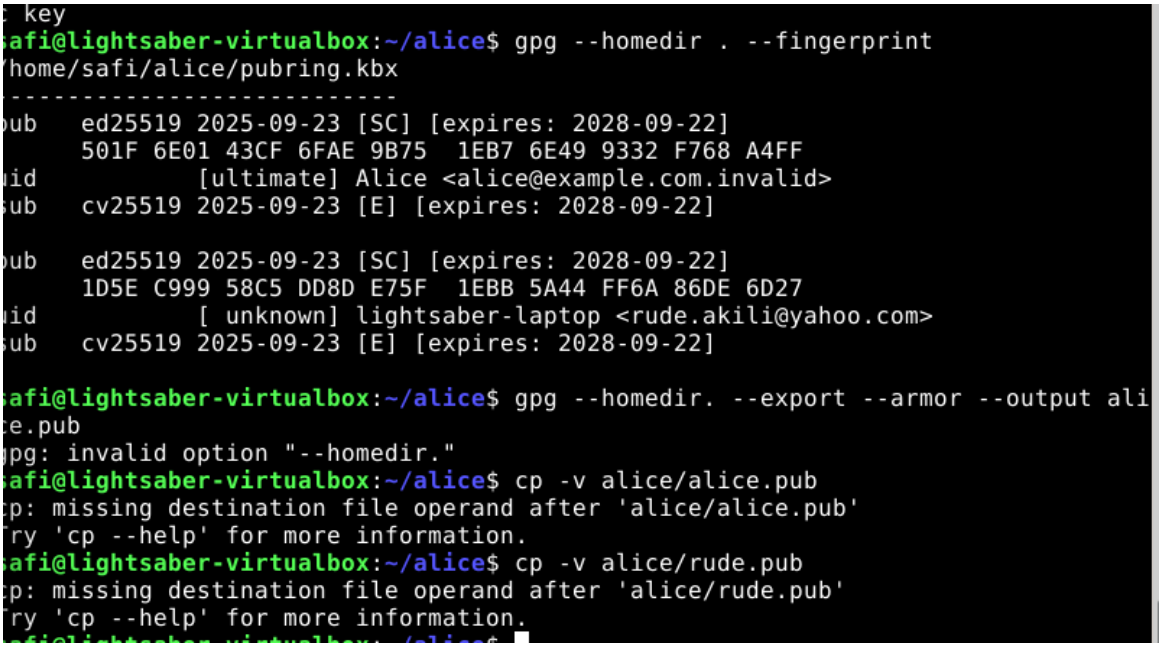
PGP

- GNU: privacy guard for gpg, a popular encryption way and sign

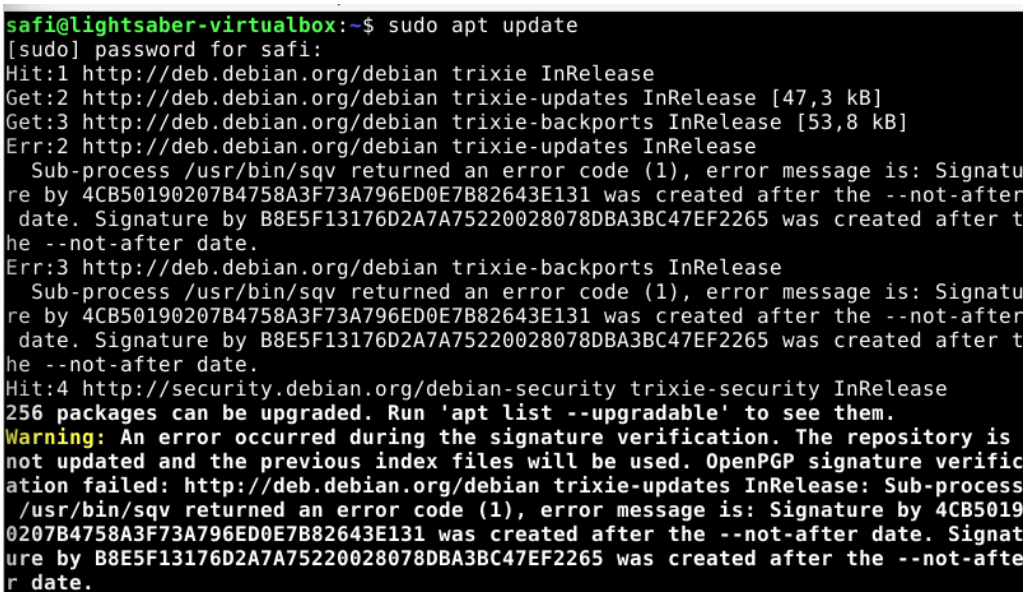








I managed to create Alice in the linux but couldn't fix the issue with the files missing. Therefore I couldn't finish with encrypting and decrypting a message between the two.



I've come across an issue when trying to update my VM to download the password manager.

Password managers are important because you can create more complicated passwords and protect against keyloggers. Keyloggers are logs that have been recorded from the used characters. This is a common way to steal someone's password.

It can manage ssh keys and keep it private and create backups.