My Name-Surname: Barış KAPLAN - My KU ID Number: 0069054
My KU ID Number: 0069054 (69054)
My KU Email Address: bkaplan18@ku.edu.tr
The Project Number: Project #1
Term: Spring 2022
Lecture Name: COMP434

My Answers:

1-) The hashes of the passphrases are utilized in the process of encrypting the private keys. In addition to that, passphrases are utilized in the processes of decrypting and then using these private keys. By using the hash of the passphrases in these processes to encrypt the private keys, we disable the access of attackers to the private keys. The passphrase should minimumly involve 15 charachters (Note: 15 charachters roughly correspond to 4 words). A password should minimumly involve 8 charachters. When we compare the number of possible amount of letter tries for guessing a password and for guessing a passphrase in the worst case, we can see that the number of letter tries to guess a passphrase is much larger. (15!=1.3 * 10^12 , 8!= 40320, 40320<<1.3 * 10^12) . From this situation, since the minimum length of a passphrase is bigger than a password, we can reach a conclusion that guessing a passphrase is usually harder than guessing a password for the attacker. So, having a passphrase usually provides more security than having a password. Moreover, passphrases prevents the possible cyber attacks , and decreases the vulnerabilities of a system more than passwords. In the passphrase, we can use  commonly used words as the sub-phrases. When we use commonly used words in the passphrases, then there needs to be several dictionary attacks to obtain the passphrase (Several dictionary attacks correspond to O(n^2) time complexity where n represents the length of the dictionary and the length of salt values of the dictionary items. In a dictionary attack; hashing each item in the dictionary needs O(n) time complexity, where n is the length of the dictionary.). We can also make our passphrases from some uncommon words and multiple types of charachters (uppercase letters, lowercase letters, numbers, punctuations, symbols, unicode charachters, and so on). In that case, an attacker should do much more dictionary attacks and additional research in order to obtain the passphrase. So, this situation provides much more security to the passphrases. Moreover; the letters and words in a passphrase can be more randomized and disordered in a passphrase, which makes using a passphrase more secure than using a password. Using passphrases instead of passwords also makes the attacks to our systems/mail accounts/applications more difficult. In the Pretty Good Privacy (PGP) Program, the passphrases are utilized in the process of decrypting a mail/message and signing a mail/message. Passphrases are also used to secure the applications which controls some company-related and/or personal passwords. While deciding the passphrases; we should make sure that the words in the passphrases do not include our personal information, and they do not include consecutive charachters multiple times. Overall; we use passphrases to make our systems/applications/email accounts much more secure, to decrease the vulnerabilities in our systems/applications/email accounts more, and to diminish the number of possible cyber attacks to our systems/applications/email accounts more. The length of the passphrases are more than the length of the passwords. Moreover, a passphrase can be more randomized and disordered than a password. So, for the attacker; it is harder to guess a passphrase in comparison to a password (For minimum number of letters in a passphrase and in a password; in the worst case, it tooks 15! letter guesses for the passphrases, and 8! letter guesses for the passwords. 15!>>8!. Length takes a significant role in securing the systems! ).

2-) It is more possible to capture and/or crack the keys that do not expire never. When the keys do not expire never, there exists only one alternative of key to access at all times (for the attacker). Hence, it is easy for attacker to do attacks, and access & crack the keys. However; if the key has an expiration time; an attacker should apply more attacks in order to reach the constantly resetted key, and has several key alternatives to try. Thus, it will be harder for the attacker to access and/or crack the key. In order to increase the security of the systems & applications & email accounts, we should keep the key expiration date updated as much as possible, and should not keep the key expiration time long. If we set the key expiration time short, then our key on a keyserver (such as: https://keys.openpgp.org/) will become unusuable and invalid constantly. This situation makes us to constantly update our key on the keyservers, decrease the cybersecurity vulnerabilities more, and prevent malicious cyber attacks launched against to our email accounts/systems/applications more. If we keep the key expiration time long, then in terms of security, our systems will be more vulnerable. Moreover, the key access/crack will be more possible. If the key expiration time is set to be earlier than the key access/crack time, then having a key expiration date can prevent malicious attacks to this key. This situation will increase the security of the system which uses that particular key. Nonetheless, if we are constantly able to access our private keys and our key revocation certificate; then in terms of security, having a key expiration time and not having a key expiration time have identical influences on the key.

3-) Revocating a key is the process of taking the accessed and/or obtained keys out. By using the private key and its' passphrase, we can revoke the key. If we cannot remember the passphrase of the private key and/or lost the private key, we want to immediately make the key unusuable and invalid. For the aim of making the key unusable and invalid; key revocation certificates can help us and can increase the security of the systems by managing and controlling the keys.

4-) Encryption and signing require two non-identical keys in order to decrease the possibility of accessing to our documents by someone except us. By accessing to the private encryption key, an attacker can read the contents of the encrypted documents/mails. Nonetheless, he/she cannot utilize this key to digitally sign a mail/document. In addition to these; in order to prevent cyber attacks (especially the eavesdropping attacks, the alteration attacks, and the denial-of-service attacks) to our email account/system and to diminish the cybersecurity vulnerabilities in our email account/system, we utillize different keys in encrypting and signing. We can also prevent possible data breaches by utilizing different keys for encryption and signing. As an another reason, having two different keys for encrypting and signing enables to have non-identical key expiration times for the processes of signing and encrypting. Moreover; since we want to ensure & strenghten the non-repudiation (non-repudiation means that a person is not able to deny a digitally signed document/message by himself/herself.) concept in security, we use different keys for encryption and signing. Finally, since we want to obey & apply the confidentiality, integrity, availability, and authenticity goals of the security, we use non-identical keys for encryption and signing.

5-) No, the email titles are not encrypted. One of the possible consequences is the impersonation of the email sender. By copying our identity number, an attacker can easily reach our personal information (personal information such as mother name, father name, serial number, birth place, our name-surname, and so on) and impersonate us. Another possible consequence is that the money in our bank account / bank accounts can be transferred into the bank account of the attacker. An attacker can see the password of our bank account, copy it to somewhere available to her/him, and maybe distribute to his/her friend involved in the process of transferring money. As a third consequence, possible data breaches in a company can result in the decrease of the reputation of a company in the markets in which this company is involved. If the personal knowledge of a customer of this company is leaked (even partly), then the customer decreases his/her trust on that company. When a customer decreases his/her trust to a company, then this customer most probably start to buy the products from, and/or benefit from the services of a different company. For the company to which the trust of the customer decreases; this can also lead to the decreases in sales volume, sales revenue, and sales profit. The security goals involve availability, integrity, and confidentiality. As a fourth result, when our personal information is stolen by an attacker, the security goals are violated by this attacker. In the security goals, confidentiality is a concept which means making the attackers and/or any other unauthorized people cannot reach the personal & the other private information of us. The confidentiality principle saves the personal & other private information of us against the attackers. Furthermore; if our identity information is obtained by the attacker, then there will be an illegal & unauthorized authentication of us (authentication is done by the attacker). Moreover, unencrypted email titles may lead to the alteration and distribution of our personal information (alteration and distribution processes are performed by the attacker). The possible unauthorized alteration of our personal & the other private information of us (causes violation in the integrity) means that a possible violation in integrity goal of the security can occur. According to the availability goal of the security, the personal and/or private information should not be available to the unauthorized people, and to the attackers. In addition, these personal information should be easily reachable by the authorized people. By considering this, we can say that another possible consequence of unencrypted email titles is the violation in the availability goal of the security.