UiO : Department of Informatics
University of Oslo

DIGHEL4360 – Autumn 2023

Workshop - Security II

Obligatory tasks, submission deadline: 30. October

Task 1

You have eavesdropped a communication encrypted with the Caesar cipher:

VAPELCGBTENCULNPNRFNEPVCURENYFBXABJANFGURFUVSGPVCUREPNRFNEPBQRBEPNRFNEF
UVSGVFBARBSGURFVZCYRFGNAQZBFGJVQRYLXABJARAPELCGVBAGRPUAVDHRF

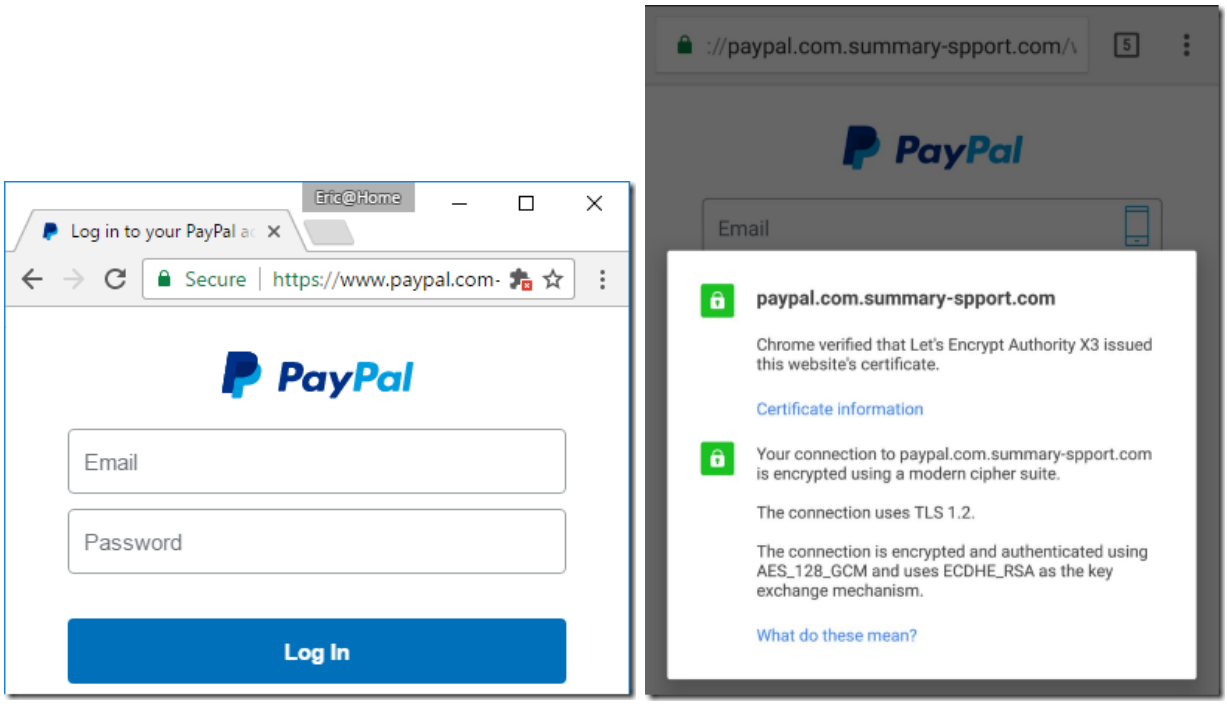
Try to decode the message. Use for example the online tool https://cryptii.com/pipes/caesar-cipher, switch to "DECODE" and test the different possibilities. What is the decryption key?

Task 2

Go to "ruter.no" and check the details of the connection.

1. Does the server use TLS / HTTPS?
2. If yes, which TLS version (1.x) is used? Which bit length is used with AES? What is the name of the certificate authority that created the certificate for ruter.no?

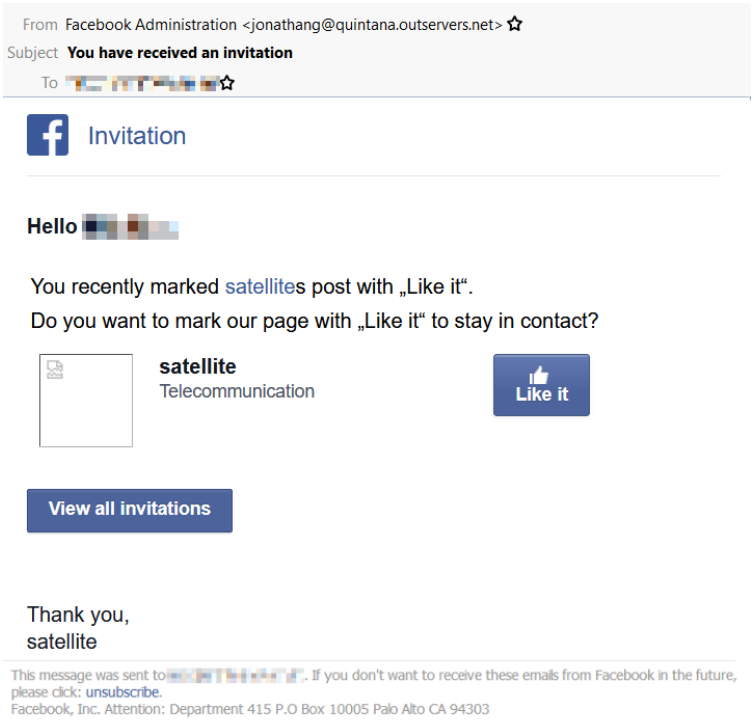
Task 3



You received a reminder from PayPal to update your user profile. You open the link and see the Web page shown on the screen shots.

1. Is this the genuine PayPal Web page?
2. Is the page using HTTPS? What does HTTPS imply regarding the security of the communication?
3. Does the page have a certificate? Is the certificate valid?
4. What can you conclude from the observations above about HTTPS and the security of a Web page?

Task 4



1. Look at the email shown in the figure. You have the suspicion that it is a phishing email. What caught your suspicion? (Ignore the two blurred bars; assume your own name/email address is shown there.)
2. What information (not visible in the picture) should you check next?
3. It seems, that the image was not loaded by the email program. You click the button "show external images" to see the whole email. Is this a good idea? Why/why not?