Links E2EE

הדגשות: **חשוב ביותר** **מועיל מאוד** רגיל פחות חשוב

למרות ההשקעה המשמעותית באיסוף הקישורים וסינונם, לא בטוח שהם הטובים ביותר!

מימוש פרוטוקול דומה(אבל שונה) בעברית עם הקוד **בפייתון**(הקישור לגיט שבסוף אינו תקין):
https://digitalwhisper.co.il/files/Zines/0xA1/DW161-3-E2EEncryption.pdf

General explanation: https://www.preveil.com/blog/end-to-end-encryption

Wiki: https://en.wikipedia.org/wiki/End-to-end_encryption

Good explanation(IBM): https://www.ibm.com/topics/end-to-end-encryption

Differences from alike: https://blog.cubbit.io/end-to-end-encryption-explained

Steps in general: https://myasir360.medium.com/implementing-end-to-end-encryption-in-messaging-apps-a-step-by-step-guide-aa4fed09bdb7

One more: https://www.preveil.com/blog/end-to-end-encryption/#:~:text=End%2Dto%2Dend%20encryption%20example,-Let's%20take%20an&text=Bob%20wants%20to%20send%20Alice,encrypted%20message%20to%20Alice's%20device

Step by step in short: https://www.kiteworks.com/secure-file-sharing/real-world-examples-of-end-to-end-encryption

With vulnerabilities: https://www.aciworldwide.com/end-to-end-encryption

MITM: https://security.stackexchange.com/questions/211828/man-in-the-middle-attacks-in-end-to-end-encryption

Profound, too complicated: https://www.qed42.com/insights/developing-a-real-time-secure-chat-application-like-whatsapp-signal-with-end-to-end-encryption

Python implementations: https://medium.com/@maxel333/asymmetric-encryption-understanding-end-to-end-encryption-e2ee-in-python-a9abcf1d157

https://medium.com/@halildeniz313/unlock-the-power-of-end-to-end-encryption-with-python-85a199b4f18f

https://denizhalil.com/2024/05/27/end-to-end-encryption-python

Git: https://github.com/anishvedant/End-to-End-Encryption

Many steps implemented: https://github.com/geniuszlyy/GenE2EETool

E2EEchat(no need to implement): https://github.com/ludvigknutsmark/python-chat

E2EE Messaging implementation:
https://libraetd.lib.virginia.edu/downloads/3b5919466?filename=Yelisetty_Rithik_Prospectus.pdf

Some Python functions: https://iha089.org.in/end-to-end-encryption-with-python

Whatsapp: https://ocw.cs.pub.ro/courses/ac/laboratoare/08
https://ocw.cs.pub.ro/courses/ac/laboratoare/09

Python crash course: https://ocw.cs.pub.ro/courses/ac/laboratoare/01

Possible Attacks
https://arminstraub.com/downloads/teaching/cryptography-spring17/lecture32.pdf
https://github.com/Akhi-99/Attacks-on-RSA
https://crypto.stackexchange.com/questions/2323/how-does-a-chosen-plaintext-attack-on-rsa-work
https://asecuritysite.com/encryption/c_c

Decoder
https://www.dcode.fr/rsa-cipher
https://github.com/ihebski/factordb

Key derivation- password/passphrase length(on the page 11):
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf
https://www.ssh.com/academy/ssh/passphrase

Public exponent(enough to read one and understand what and why is important):
https://en.wikipedia.org/wiki/RSA_(cryptosystem)
https://stackoverflow.com/questions/6098381/what-are-common-rsa-sign-exponent
https://crypto.stackexchange.com/questions/18031/how-to-find-modulus-from-a-rsa-public-key