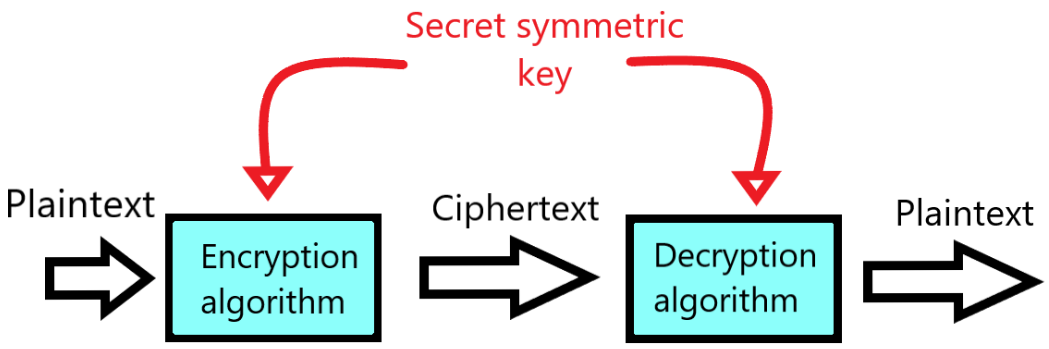
SRP Lab 2



- Koristili smo Brute-force napad kako bismo otkrili tajni ključ za dekriptiranje ciphertexta
- Svatko je imao personalizirani plaintext koji je enkriptiran korištenjem Fernet sustava
- Moj ciphertext se zvao "ba5f3913296ffec27830442870341d7ae787c8f5d761c1628355b049c4503bbe.encrypted"
- Linije koda koje sam koristio u Visual Studio Code-u:

```
import base64
from cryptography.fernet import Fernet
def brute_force():
filename="ba5f3913296ffec27830442870341d7ae787c8f5d761c1628355b049c4503bbe.encrypted"
with open(filename, "rb") as file:
ciphertext = file.read()
ctr = 0
while True:
key_bytes = ctr.to_bytes(32, "big")
key = base64.urlsafe_b64encode(key_bytes)
try:
```

```
fernet = Fernet(key)
plaintext=fernet.decrypt(ciphertext)
print(key, plaintext)
break
except Exception:
pass
ctr += 1
if __name__ == "__main__":
brute_force()
```