

1. Generowanie klucza RSA

```
openssl genrsa -out private.pem 2048
```

```
openssl rsa -in private.pem -pubout -out public.pem
```

```
└─(kali㉿kali)-[~/Documents/Projekt]
$ openssl genrsa -out private.pem 2048

└─(kali㉿kali)-[~/Documents/Projekt]
$ openssl rsa -in private.pem -pubout -out public.pem
writing RSA key

└─(kali㉿kali)-[~/Documents/Projekt]
$ █
```

2. Szyfrowanie kluczem

```
echo "Sekret OpenSSL" > dane.txt
```

```
openssl pkeyutl -encrypt -pubin -inkey public.pem -in dane.txt -out dane.enc
```

```
└─(kali㉿kali)-[~/Documents/Projekt]
$ openssl pkeyutl -encrypt -pubin -inkey public.pem -in dane.txt -out dane.enc
```

3. Sprawdzenie zaszyfrowanego pliku

```
└─(kali㉿kali)-[~/Documents/Projekt]
$ cat dane.enc
J♦♦c♦I♦/w7&H
♦y♦♦KJ♦x7w]♦\♦y♦♦♦7jB♦j♦F+♦♦♦"-
♦Z(♦♦♦♦V♦`♦♦G♦'♦Y♦█♦♦♦♦r L♦♦♦♦e♦[♦d0♦♦♦=♦WRI♦♦♦♦E█PV♦♦k♦@}56♦♦A♦♦♦S♦♦Ù♦♦
```

4. Deszyfrowanie kluczem publicznym

```
openssl rsautl -decrypt -inkey private.pem -in dane.enc -out dane_dec.txt
```

```
└─(kali㉿kali)-[~/Documents/Projekt]
$ openssl pkeyutl -decrypt -inkey private.pem -in dane.enc -out dane_dec.txt
```

5. Sprawdzenie pliku

```
Cat dane_dec.txt
```

```
└─(kali㉿kali)-[~/Documents/Projekt]
$ cat dane_dec.txt
Sekret OpenSSL
```

