

zad1

Task 1	✔	What will this room cover?	▼
Task 2	✔	Key terms	▼
Task 3	✔	Why is Encryption important?	▼
Task 4	✔	Crucial Crypto Maths	▼
Task 5	✔	Types of Encryption	▼
Task 6	✔	RSA - Rivest Shamir Adleman	▼
Task 7	✔	Establishing Keys Using Asymmetric Cryptography	▼
Task 8	✔	Digital signatures and Certificates	▼
Task 9	✔	SSH Authentication	📄 ▼
Task 10	✔	Explaining Diffie Hellman Key Exchange	▼
Task 11	✔	PGP, GPG and AES	📄 ▼
Task 12	✔	The Future - Quantum Computers and Encryption	🗨️

zad 2

Plik do zaszyfrowania

```
kamilslimak@kamilslimaks-macbook~/lab12> cat text.txt
Lorem ipsum dolor sit amet, consectetur adipiscing elit. In cursus mattis orci. Curabitur vel mi ut magna lobortis auctor. Maecenas diam libero, aliquet quis enim in, tristique euismod turpis. Praesent lacinia urna posuere enim luctus mollis. Sed commodo lacinia tellus nec tristique. Praesent ut nulla id tellus tincidunt elementum. Nulla convallis faucibus rhoncus. Quisque leo dolor, mollis sit amet tincidunt at, aliquam vitae orci. Donec ullamcorper nulla a purus hendrerit accumsan. Proin sollicitudin fermentum orci a porttitor. Morbi sit amet hendrerit quam.

Nullam at sem pharetra, scelerisque erat nec, commodo urna. Praesent id dolor tincidunt, congue turpis quis, sagittis nisi. Integer egestas enim at arcu euismod ullamcorper. Curabitur venenatis massa purus, ac gravida arcu cursus sed. Vestibulum non elementum dolor, a placerat justo. Aenean tincidunt suscipit facilisis. Aenean hendrerit dignissim feugiat. Pellentesque quis erat eros. Vestibulum fermentum tincidunt dui quis consequat. Mauris mollis efficitur ipsum quis efficitur. Donec est velit, mattis non maximus et, suscipit quis purus. Nam aliquet egestas est, id pretium mi pharetra ac.
```

Wykonanie skryptu

```
kamilslimak@kamilslimaks-macbook~/lab12> ./aes.sh text.txt "haslo"
```

Zaszyfrowany plik:

```
kamilslimak@kamilslimak-macbook~/lab12> cat output.txt
Salted____m??MT?[?????L???
_#?pgA9??{??O?S??D?CtK??}dd????J??      ?a??Y3?m??c#??
                                ?c?z?: ??  ?{?2nE|?J?'4[??????A?${?x? +?ó>?|??J8|2
Nli?p?M~???i9?u?? :0?
                                ?x?v?6?s?????-b1?{?>k?[%i?? "????8??@osC_?????ie$6?Pa/?S?? }??4C}??b?????????? ,?S{?
? T0?g>.??%:-???>      \???/??K6?W?!k??b?????:fPe?"??y?U?σ÷??h?%?a?
0??z#?83iW"?z??Cv?V??hC:x???E?u???      ?0B      i??
                                ??xg?;
???HUL?9?h?r?????0?R.? [ ?? ,i?9%M???????@?cS?[l??:L??n
???,?C?vb?? ,?m??j4?y?c???X????f?X??7
?5(?omM???e≤W?[<?J??;????*????73??u?z?y??}=?T[?(?E? ?= ?? :ol?:?'`a?ť?ah???W?od??\?6b?%?Q/?
                                r??H?????6?[??Y
?=?0V:???·?. ??????????K<?0????X
                                ?f^<???+3????LF?v; ??a?t\Q?ö?2s%???????)?P?%?Q??Eq?e_????????3?_?m???m@
ax?\[??P;;o
?L[+?"???J?#H??\?s??@?E??KT.?y$Q?
                                ?????????f?W/0????\}?/?M??9?????xP0%?z0?f??j?G??n?????>lf?;????????????
???cH4?m?G?A?j??
                                ??9?????]t??+?? 76?9??{?g?l(?????? ?q`X~?
                                SsL~k?)???:|d??H|???i?@Q?(???I?!tB\???.?
$???@??F?(L-???9x"???@vkiC???f?????E?v6pyW.ec?j)?'LX??!??j6"??y:??2?k?.????
                                ???3R
```

skrypt aes.sh:

```
#!/bin/bash

openssl enc -aes-256-cbc -salt -pbkdf2 -iter 10000 -in "$1" -out "output.txt" -k "$2"

~
~
~
~
~
```

zad 3

tworzenie kluczy prywatnego i publicznego

```
kamilslimak@kamilslimak-macbook~/lab12> openssl genrsa -aes128 -passout pass:kamil123 -out private.pem 2048
kamilslimak@kamilslimak-macbook~/lab12> openssl rsa -in private.pem -passin pass:kamil123 -pubout -out public.pem
```

sign.sh:

```
#!/bin/bash

filename=$1
privatekey=$2

if [[ $# -lt 2 ]] ; then
    echo "Usage: sign <file> <private_key>"
    exit 1
fi

openssl dgst -sha256 -sign $privatekey -out /tmp/$filename.sha256 $filename
openssl base64 -in /tmp/$filename.sha256 -out signature.sha256
rm /tmp/$filename.sha256

~
~
~
```

użycie:

```
kamilslimak@kamilslimaks-macbook~/lab12> ./sign.sh example file.txt private.pem
Enter pass phrase for private.pem:
kamilslimak@kamilslimaks-macbook~/lab12> █
```