Q1

The output of Q1

```
┌──(root㉿kali)-[~]
└─# gcc q1.c

┌──(root㉿kali)-[~]
└─# ./a.out
abcd
abce
abcf
abcg
abch
abci
abcj
abck
abcl
abcm
abcn
```

```
zyxm
zyxn   gcc decryptKey.c -lcrypto
zyxo
zyxp
zyxq   encryptRSA.o -lcrypto -o encryptRSA
zyxr   /bin/ld: cannot find encryptRSA.o: No such file or directory
zyxs   cc1: error: ld returned 1 exit status
zyxt
zyxu
zyxv
zyxw
Total combinations: 358800
```

```
┌──(root㉿kali)-[~]
└─# echo "$((26 * 25 * 24 * 23))"
358800
```

Q2

Task1: The output of task1 of Q2

```
┌──(root㉿kali)-[~]
└─# gcc q2t2.c -lcrypto

┌──(root㉿kali)-[~]
└─# ./a.out
Private key (d): C5148B1AD7C6D85847C52EABB879F26CCCEE8EB70D2282DC6050309C18F85D85
```

Task2: The output of task2 of Q2

```
┌──(root㉿kali)-[~]
└─# vim decryptKey.c

┌──(root㉿kali)-[~]
└─# gcc decryptKey.c -lcrypto

┌──(root㉿kali)-[~]
└─# ./a.out
Enter your Encrypted Message:
858FF93C7C313EDC14E79A13EAF539D0893DACC7C70D335384965088E88AFC

Original Message:
Congratulation you solved it.
```

Encrypt messages by the attached file encryptRSA.o

```
Need to get 3386 kB of archives.
After this operation, 8188 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libssl1.1 amd64 1.1.1w-0
Get:2 http://deb.debian.org/debian bullseye/main amd64 libssl-dev amd64 1.1.1w-
Fetched 3386 kB in 3s (1040 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
(Reading database ... 45424 files and directories currently installed.)
Preparing to unpack .../libssl1.1_1.1.1w-0+deb11u1_amd64.deb ...
Unpacking libssl1.1:amd64 (1.1.1w-0+deb11u1) over (1.1.1n-0+deb11u5) ...
Setting up libssl1.1:amd64 (1.1.1w-0+deb11u1) ...
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 45424 files and directories currently installed.)
Preparing to unpack .../libssl-dev_1.1.1w-0+deb11u1_amd64.deb ...
Unpacking libssl-dev:amd64 (1.1.1w-0+deb11u1) ...
Setting up libssl-dev:amd64 (1.1.1w-0+deb11u1) ...
Processing triggers for libc-bin (2.31-13+deb11u6) ...
Enumerating objects: 1702, done.
Counting objects: 100% (1702/1702), done.
Compressing objects: 100% (1041/1041), done.
Writing objects: 100% (1702/1702), done.
Total 1702 (delta 139), reused 1673 (delta 124), pack-reused 0
root@lamp ~# gcc encryptRSA.o -lcrypto -o encryptRSA
root@lamp ~# ./encryptRSA

Enter Original Message:
King Abdulaziz University

Encoded Message:
4b696e6720416264756c617a697a20556e6976657273697479

Re-enter Encoded Message:
4b696e6720416264756c617a697a20556e6976657273697479

Encrypted Message:
0D0E0218FA3056DF66689798745DA5F05A11EDD8BA532622DB530787BAF72E2D
root@lamp ~#
```

```
┌──(root㉿kali)-[~]
└─# gcc encryptRSA.o -lcrypto -o encryptRSA

┌──(root㉿kali)-[~]
└─# ./encryptRSA

Enter Original Message:
King Abdulaziz University

Encoded Message:
4b696e6720416264756c617a697a20556e6976657273697479

Re-enter Encoded Message:
4b696e6720416264756c617a697a20556e6976657273697479

Encrypted Message:
0D0E0218FA3056DF66689798745DA5F05A11EDD8BA532622DB530787BAF72E2D

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# ./encryptRSA

Enter Original Message:
Alaa Sunbul on EE463

Encoded Message:
416c61612053756e62756c206f6e204545343633

Re-enter Encoded Message:
416c61612053756e62756c206f6e204545343633

Encrypted Message:
BD081E99381175CA9B45CEAF63C5532B4E0462FD72A36F7EC1898F47ADEA70E6

┌──(root㉿kali)-[~]
└─#
```