EE463Lab assignment

Name: Amer Khalid

ID: 1855601

Q1 code:

```
#include <stdio.h>

int main(int argc, char* argv[]) {
    char letters[] = "abcdefghijklmnopqrstuvwxyz";
    int count = 0;

    for (int i = 0; i < 26; ++i) {
        for (int j = 0; j < 26; ++j) {
            if (j == i) continue;
            for (int k = 0; k < 26; ++k) {
                if (k == i || k == j) continue;
                for (int l = 0; l < 26; ++l) {
                    if (l == i || l == j || l == k) continue;
                    printf("%c%c%c%c\n", letters[i],
letters[j], letters[k], letters[l]);
                    count++;
                }
            }
        }
    }

    printf("Total combinations: %d\n", count);

    return 0;
}
```

Q1 output:

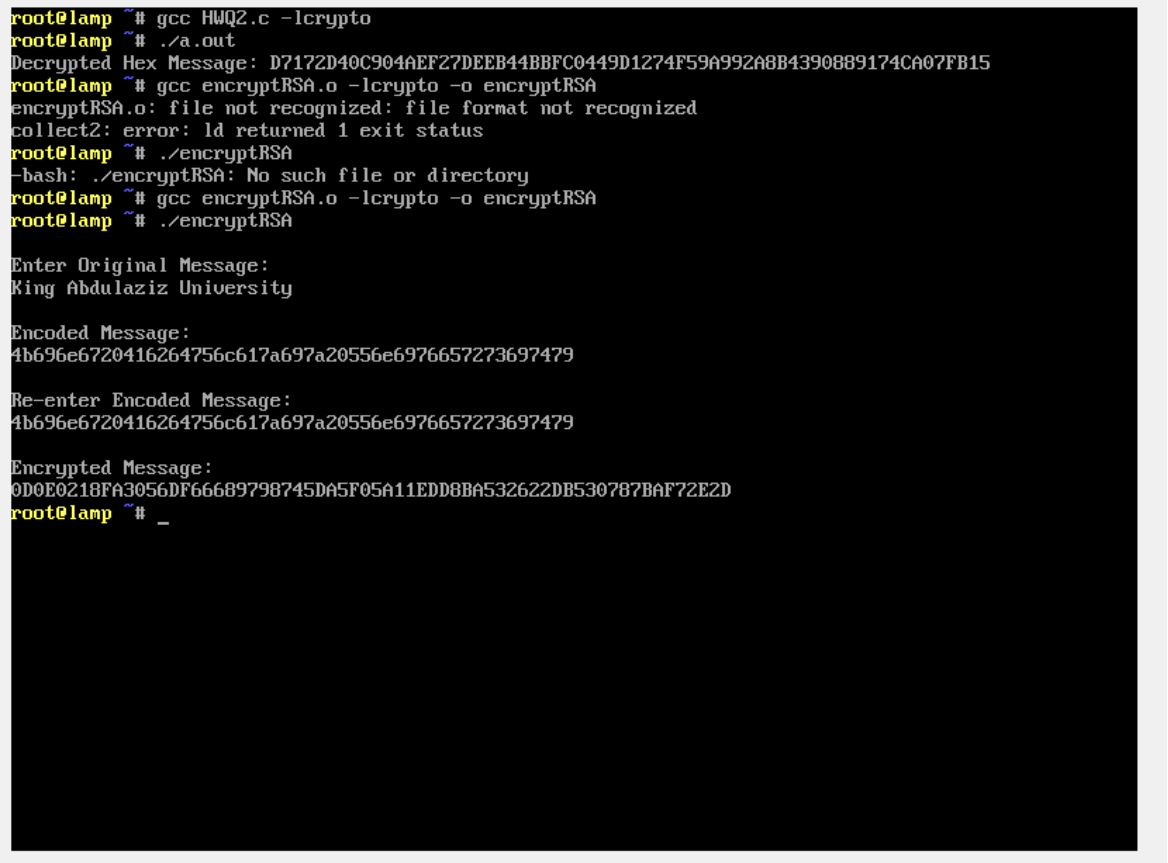
```
ezsi
ezsj
ezsk
ezsl
ezsm
ezsn
ezso
ezsp
ezsq
ezsr
ezst
ezsu
ezsv
ezsw
ezsx
ezsy
ezta
eztb
eztc
eztd
eztf
eztg
ezth
ezti
eztj
eztk
eztl
eztm
eztn
ezto
eztp
eztq
eztr
ezts
eztu
^\Quit
root@lamp ~#
```

```
zywl
zywm
zywn
zywo
zywp
zywq
zywr
zyws
zywt
zywu
zywv
zywx
zyxa
zyxb
zyxc
zyxd
zyxe
zyxf
zyxg
zyxh
zyxi
zyxj
zyxk
zyxl
zyxm
zyxn
zyxo
zyxp
zyxq
zyxr
zyxs
zyxt
zyxu
zyxv
zyxw
Total combinations: 358800
root@lamp ~#
```

Q2 code:

```
#include <stdio.h>
#include <openssl/bn.h>
#include <stdlib.h>

void printBN(char *msg, BIGNUM *tmp) {
    char *number_str = BN_bn2hex(tmp); // Convert BIGNUM to
hex
    printf("%s%s\n", msg, number_str); // Print hex
    OPENSSL_free(number_str); // Free memory
}

int main(int argc, char *argv[]) {
    BN_CTX *ctx = BN_CTX_new();

    BIGNUM *d = BN_new();
    BIGNUM *n = BN_new();
    BIGNUM *C = BN_new();
    BIGNUM *D = BN_new();

    // Assign values to n and C from hex strings
    BN_hex2bn(&n,
"E103ABD94892E3E74AFD724BF28E78366D9676BCCC70118BD0AA1968DBB14
3D1");
    BN_hex2bn(&C,
"858FF93C7C313EDC14E79A13EAF539D0893DACC7C70D335384965088E88AF
C");

    // Assign the calculated private key (d) from Task 1
    BN_hex2bn(&d,
"626C9D41C42C502A94D9078FFB8DE45A6BC97A3FA1D9E9D22DF82F35DEEA7
69");

    // Decrypt ciphertext using D = C^d mod n
    BN_mod_exp(D, C, d, n, ctx);

    // Convert the decrypted BIGNUM to a hex string and print
it
    char *decrypted_hex = BN_bn2hex(D);
    printf("Decrypted Hex Message: %s\n", decrypted_hex);

    // Free allocated memory
    BN_CTX_free(ctx);
    BN_free(d);
    BN_free(n);
    BN_free(C);
    BN_free(D);
    OPENSSL_free(decrypted_hex);

    return EXIT_SUCCESS;
}
```

Q2 output:


root@lamp ~# gcc HWQ2.c -lcrypto
root@lamp ~# ./a.out
Decrypted Hex Message: D7172D40C904AEF27DEEB44BBFC0449D1274F59A992A8B4390889174CA07FB15
root@lamp ~# gcc encryptRSA.o -lcrypto -o encryptRSA
encryptRSA.o: file not recognized: file format not recognized
collect2: error: ld returned 1 exit status
root@lamp ~# ./encryptRSA
-bash: ./encryptRSA: No such file or directory
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 ~# _