Program27 C program for Bob uses the RSA cryptosystem with a very large modulus n

#include <stdio.h>

#include <stdint.h>

uint64\_t mod\_pow(uint64\_t base, uint64\_t exponent, uint64\_t modulus)

{

uint64\_t result = 1;

base = base % modulus;

while (exponent > 0)

{

if (exponent % 2 == 1)

{

result = (result \* base) % modulus;

}

exponent >>= 1;

base = (base \* base) % modulus;

}

return result;

}

int main()

{

uint64\_t n = 12345678901;

uint64\_t e = 65537;

uint64\_t d = 123456789;

int i;

char message[] = "HELLO";

int message\_length = sizeof(message) - 1;

printf("Original Message: %s\n", message);

printf("Encrypted Message: ");

for (i = 0; i < message\_length; i++)

{

uint64\_t encrypted = mod\_pow(message[i] - 'A', e, n);

printf("%llu ", encrypted);

}

printf("\n");

printf("Decrypted Message: ");

for (i = 0; i < message\_length; i++)

{

uint64\_t encrypted = mod\_pow(message[i] - 'A', e, n);

uint64\_t decrypted = mod\_pow(encrypted, d, n) + 'A';

printf("%c", (char)decrypted);

}

printf("\n");

return 0;

}

OUTPUT:

Original Message: HELLO

Encrypted Message: 6993215515 0 5432380226 5432380226 1150641087

Decrypted Message: ]AeeK