Title	Assignment 1
Module	**M.Sc. Fundamentals of Cybersecurity**
Module Code	CP70045E
Module Leader:	**Ferda Sonmez**
Full Name/ Student Number for All Group Members:	**Sonam Tamang- 33141528** **Bishal Thapa- 33143315**
Group Name	**Group_SB**

Question 1- Implementing RSA key generation algorithm

A. Background

Rivest–Shamir–Adleman (RSA) encryption is one of the oldest and most widely used public-key cryptography approaches and introduce in 1977, it is based on modular arithmetic and the mathematical properties of huge prime numbers (Adleman, et al., 2021). RSA is required for current cryptography for secure data transport, digital signatures, and key exchange. The factoring problem for large composite integers is the foundation of RSA. A public key is used for encryption, and a private key is used for decryption, forming a dual-key scheme. The two enormous prime numbers that are used to produce these keys are kept secret. The simplicity of multiplying two enormous prime numbers—but the computational impracticability of decomposing their product to reveal the original primes is what gives RSA its potency.

Prime numbers play an important part in the creation of RSA keys. The public key, $n = p \times q$, has been calculated from two distinct huge prime numbers (p and q). Utilizing the totient function $\varphi(n) = (p-1)(q-1)$, the private key is obtained. The selection of the encryption exponent e ensures that $\gcd(e, \varphi(n)) = 1$ and that $1 < e < \varphi(n)$. The equation $d \times e \equiv 1 \pmod{\varphi(n)}$ is obtained by computing the decryption key d as the modular multiplying inverse of e with respect to $\varphi(n)$. Modular exponentiation applies in RSA operations. It guarantees efficient and safe encryption (c = m^e mod n) and decryption (m = c^d mod n) for huge integers (Vollala, et al., 2021). It also protects against overflow and ensures security through avoiding direct calculation with huge exponentiated numbers.

Question 1- B task1.c

```
┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$ ./task1
Generated prime p =  D21A4446555933ED35FF1780B42323F8008239965F8FE4334EF93253315DDB9B
Generated prime q =  DF4498AC0104938380BF183FF7050E1DE904394686938904050FF68BDFF21B83
Modulus N =  B73D2DC02A0CDD9A158D41E6CB93755D5A8069382BBF91A4EDCC7ADD7BF37B13969EDD2EEA1AE7A66C67B12C2F
CC4DBBE47D0E1CA47E49CFA08B22F5C6B6B951
Euler's Totient φ(N) =  B73D2DC02A0CDD9A158D41E6CB93755D5A8069382BBF91A4EDCC7ADD7BF37B11E540003C93BD203
5B5A9816B84A41BA5FAF69B3FBE5ADC984C81FA16B566C234
Public exponent e =  010001
Private exponent d =  5DA74F32E04B231815DBD4CAF951ACB2C206CFC07DDBB3BCF02D8ABE9913A0DB4CA8A17654AC5D421
64F446E87A4B8DCE4A0164946297A85FCD491D5F97143E1

┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$
```

Figure 1: task1.c output showing public key and values.

RSA key pairs are created by picking big prime integers, which are then used to compute key components such as the modulus, totient, public exponent, and private exponent. Two prime integers are multiplied to get the modulus, and the totient affects the values of exponents used in encryption and decoding. By investigating this process, we learnt how RSA key creation ensures safe communication. RSA's strength resides in the difficulty of these huge primes, which ensures that only authorised parties may decrypt the communication. This challenge helped us grasp how cryptographic keys safeguard digital data through secure encryption.

Keys.txt

Public Key:

e: 010001

N:CF12363551C289917F64E44467DADA7C7934B1410ECF51089DA2203CF31E6794EC16E23551C7924F2D1F2FB0B525034EB61C87AF37E9C79139DCFE4F6D29C739

Private Key:

d:7FE5D0C3A8274F4F25EF8C2A50375621F1BF41085CFC6221BF3367541E1A1681411537B2707E4C918027E9044E925207CAF5CAC7C6B66C64A1AA54F8251CE88D

N:7FE5D0C3A8274F4F25EF8C2A50375621F1BF41085CFC6221BF3367541E1A1681411537B2707E4C918027E9044E925207CAF5CAC7C6B66C64A1AA54F8251CE88D

Question 2- Encrypting and Decrypting Group Name.

A. Group Name : group_SB

Question 2- B

```
┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$ ./task2
Message as BIGNUM (hex) =  67726F75705F5342
Encrypted Ciphertext C =  33C88E6C12A29DFD0EACA0A261D1EEDB67223B318B742859D1731F85C557DCAF520F24EE9E8B2
036C3606665414D71C4739252D93E1700C585C4F41C91E0F3E6
Decrypted Message (hex) =  67726F75705F5342
Decrypted Message (ASCII) = group_SB

┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$
```

Figure2: Task2.c output RSA encryption and decryption

In this task, our group (group_SB) used the produced key pairs to implement the usage of RSA encryption. This made sure that the original message was safely encrypted by demonstrating how to use the public key to convert plaintext into ciphertext. Only with the matching private key could we decrypt this encrypted data, enabling us to precisely recover the original data. We were able to understand the practical operation of RSA encryption through this experiment. Because the original material could only be accessed by authorised people who had the right decryption key, it successfully demonstrated how privacy of information is maintained. This assignment highlighted how crucial public-key cryptography is to protecting private data and thwarting illegal access.

Question 3- RSA Digital signing using OpenSSL

```
┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$ gcc task3.c -o task3 -lcrypto

┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$ ./task3
Enter modulus (N) in hex: CF12363551C289917F64E44467DADA7C7934B1410ECF51089DA2203CF31E6794EC16E23551C7924F2D1F2FB0B
525034EB61C87AF37E9C79139DCFE4F6D29C739
Enter private exponent (d) in hex: 7FE5D0C3A8274F4F25EF8C2A50375621F1BF41085CFC6221BF3367541E1A1681411537B2707E4C91
8027E9044E925207CAF5CAC7C6B66C64A1AA54F8251CE88D
Enter the message to sign: I owe group_SB $2000
Message as BIGMMU (hex): 49206F77652067726F75705F5342202432303030
Generated Signature S = A9396AC72E182CE9D04489DBD2D8535D4C514AB08D9887E06DC3A17401A03C3BA9962FBF8D92B97F6D91ECEE053
BE9C89C195FC32A3A41CC1C9CFAEB253AD839

┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$ ./task3
Enter modulus (N) in hex: CF12363551C289917F64E44467DADA7C7934B1410ECF51089DA2203CF31E6794EC16E23551C7924F2D1F2FB0B
525034EB61C87AF37E9C79139DCFE4F6D29C739
Enter private exponent (d) in hex: 7FE5D0C3A8274F4F25EF8C2A50375621F1BF41085CFC6221BF3367541E1A1681411537B2707E4C91
8027E9044E925207CAF5CAC7C6B66C64A1AA54F8251CE88D
Enter the message to sign: I owe group_SB $3000
Message as BIGMMU (hex): 49206F77652067726F75705F5342202433303030
Generated Signature S = A04833360A1745A251CA086022E09F14821F86AA094B1A2EBB9DDA4C5607AB9AE38E34AC4E4C9384F7C396052E2
2364BA2D1BF997F2C777158853CF40E3348ED
```

Figure 3: task3.c RSA to digital signature

In this task, the private key associated with a particular message was used to produce a digital signature. This procedure illustrated the creation of digital signatures to guarantee the legitimacy of the message's source. Intentionally, the original message was changed to better explore the idea. This change made it possible for us to see the effects of message manipulation and made it abundantly evident how important digital signatures are to preserving the confidentiality of digital communications. The significance of digital signatures in identifying unauthorised changes and guaranteeing safe message transmission was further supported by the comparison of the original and changed messages, which showed that any modification in the content results in a failure of the signature verification.

Question 4- RSA signature verification using OpenSSL

Figure 4: task4.c RSA signature verification by changing signature byte.

The public key is used in RSA signature verification to ensure that a message comes from the correct source and hasn't been altered. We purposefully altered the signature data to test the system's ability to detect any changes. The system's ability to consistently identify when something has been changed is demonstrated by its effective reporting of the altered message. This demonstrates how it can aid in preventing unapproved or misleading messages.

5. Decrypted text

“IT IS A TRUTH UNIVERSALLY ACKNOWLEDGED THAT A SINGLE MAN IN POSSESSION OF A GOOD FORTUNE MUST BE IN WANT OF A WIFE.”

“OWEVER LITTLE KNOWN THE FEELINGS OR VIEWS OF SUCH A MAN MAY BE ON HIS FIRST ENTERING A NEIGHBORHOOD, THIS TRUTH IS SO WELL FIXED IN THE MINDS OF THE SURROUNDING FAMILIES, THAT HE IS CONSIDERED AS THE RIGHTFUL PROPERTY OF SOME ONE OR OTHER OF THEIR DAUGHTERS.”

“MY DEAR MR. BENNET,” SAID HIS LADY TO HIM ONE DAY, “HAVE YOU HEARD THAT NETHERFIELD PARK IS LET AT LAST?”

MR. BENNET REPLIED THAT HE HAD NOT. “BUT IT IS,” RETURNED SHE, “FOR MRS. LONG HAS JUST BEEN HERE, AND SHE TOLD ME ALL ABOUT IT.”

MR. BENNET MADE NO ANSWER.

“DO YOU NOT WANT TO KNOW WHO HAS TAKEN IT?” CRIED HIS WIFE, IMPATIENTLY.

“YOU WANT TO TELL ME, AND I HAVE NO OBJECTION TO HEARING IT.”

THIS WAS INVITATION ENOUGH.

“WHY, MY DEAR, YOU MUST KNOW, MRS. LONG SAYS THAT NETHERFIELD IS TAKEN BY

A YOUNG MAN OF LARGE FORTUNE FROM THE NORTH OF ENGLAND; THAT HE CAME DOWN ON MONDAY IN A CHAISE-AND-FOUR TO SEE THE PLACE, AND WAS SO MUCH DELIGHTED WITH IT THAT HE AGREED WITH MR. MORRIS IMMEDIATELY; THAT HE IS TO TAKE POSSESSION BEFORE MICHAELMAS, AND SOME OF HIS SERVANTS ARE TO BE IN THE HOUSE BY THE END OF NEXT WEEK."

"WHAT IS HIS NAME?"

"BINGLEY."

"IS HE MARRIED OR SINGLE?"

"OH, SINGLE, MY DEAR, TO BE SURE! A SINGLE MAN OF LARGE FORTUNE—FOUR OR FIVE THOUSAND A YEAR. WHAT A FINE THING FOR OUR GIRLS!"

"HOW SO? HOW CAN IT AFFECT THEM?"

"MY DEAR MR. BENNET," REPLIED HIS WIFE, "HOW CAN YOU BE SO TIRESOME? YOU MUST KNOW THAT I AM THINKING OF HIS MARRYING ONE OF THEM."

"IS THAT HIS DESIGN IN SETTLING HERE?"

"DESIGN? NONSENSE, HOW CAN YOU TALK SO! BUT IT IS VERY LIKELY THAT HE MAY FALL IN LOVE WITH ONE OF THEM, AND THEREFORE YOU MUST VISIT HIM AS SOON AS HE COMES."

"I SEE NO OCCASION FOR THAT. YOU AND THE GIRLS MAY GO, OR YOU MAY SEND THEM BY THEMSELVES, WHICH PERHAPS WILL BE STILL BETTER; FOR AS YOU ARE AS HANDSOME AS ANY OF THEM, MR. BINGLEY MAY LIKE YOU THE BEST OF THE PARTY."

"MY DEAR, YOU FLATTER ME. I CERTAINLY HAVE HAD MY SHARE OF BEAUTY, BUT I DO NOT PRETEND TO BE ANYTHING EXTRAORDINARY NOW. WHEN A WOMAN HAS FIVE GROWNUP DAUGHTERS, SHE OUGHT TO GIVE OVER THINKING OF HER OWN BEAUTY."

"IN SUCH CASES A WOMAN HAS NOT OFTEN MUCH BEAUTY TO THINK OF."

"BUT, MY DEAR, YOU MUST INDEED GO AND SEE MR. BINGLEY WHEN HE COMES INTO THE NEIGHBORHOOD."

"IT IS MORE THAN I ENGAGE FOR, I ASSURE YOU."

"BUT CONSIDER YOUR DAUGHTERS. ONLY THINK WHAT AN ESTABLISHMENT IT WOULD BE FOR ONE OF THEM! SIR WILLIAM AND LADY LUCAS ARE DETERMINED TO GO, MERELY ON THAT ACCOUNT; FOR IN GENERAL, YOU KNOW, THEY VISIT NO NEW-COMERS. INDEED, YOU MUST GO, FOR IT WILL BE IMPOSSIBLE FOR US TO VISIT HIM, IF

YOU DO NOT."

"YOU ARE OVER-SCRUPULOUS, SURELY. I DARE SAY MR. BINGLEY WILL BE VERY GLAD TO SEE YOU; AND I WILL SEND A FEW LINES BY YOU TO ASSURE HIM OF MY HEARTY CONSENT TO HIS MARRYING WHICHEVER HE CHOOSES OF THE GIRLS; THOUGH I MUST THROW IN A GOOD WORD FOR MY LITTLE LIZZY."

"I DESIRE YOU WILL DO NO SUCH THING. LIZZY IS NOT A BIT BETTER THAN THE OTHERS; AND I AM SURE SHE IS NOT HALF SO HANDSOME AS JANE, NOR HALF SO GOOD-HUMORED AS LYDIA. BUT YOU ARE ALWAYS GIVING HER THE PREFERENCE."

"THEY HAVE NONE OF THEM MUCH TO RECOMMEND THEM," REPLIED HE. "THEY ARE ALL SILLY AND IGNORANT LIKE OTHER GIRLS; BUT LIZZY HAS SOMETHING MORE OF QUICKNESS THAN HER SISTERS."

"MR. BENNET, HOW CAN YOU ABUSE YOUR OWN CHILDREN IN SUCH A WAY? YOU TAKE DELIGHT IN VEXING ME. YOU HAVE NO COMPASSION ON MY POOR NERVES."

"YOU MISTAKE ME, MY DEAR. I HAVE A HIGH RESPECT FOR YOUR NERVES. THEY ARE MY OLD FRIENDS. I HAVE HEARD YOU MENTION THEM WITH CONSIDERATION THESE TWENTY YEARS AT LEAST."

"AH, YOU DO NOT KNOW WHAT I SUFFER!"

"BUT I HOPE YOU WILL GET OVER IT, AND LIVE TO SEE MANY YOUNG MEN OF FOUR THOUSAND A YEAR COME INTO THE NEIGHBORHOOD."

"IT WILL BE NO USE TO US IF TWENTY SUCH SHOULD COME, SINCE YOU WILL NOT VISIT THEM."

"DEPEND UPON IT, MY DEAR, THAT WHEN THERE ARE TWENTY I WILL VISIT THEM ALL." MR. BENNET WAS SO ODD A MIXTURE OF QUICK TARTS, SARCASTIC HUMOR, RESERVE, AND CAPRICE, THAT THE EXPERIENCE OF THREE-AND-TWENTY YEARS HAD BEEN INSUFFICIENT TO MAKE HIS WIFE UNDERSTAND HIS CHARACTER. HER MIND WAS LESS DIFFICULT TO DEVELOP. SHE WAS A WOMAN OF MEAN UNDERSTANDING, LITTLE INFORMATION, AND UNCERTAIN TEMPER. WHEN SHE WAS DISCONTENTED, SHE FANCIED HERSELF NERVOUS. THE BUSINESS OF HER LIFE WAS TO GET HER DAUGHTERS MARRIED; ITS SOLACE WAS VISITING AND NEWS."

Mappings.txt

```
┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$ gcc task5_1.c -o task5_1

┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$ ./task5_1

Letter Frequency Analysis (Sorted Descending):
------------------------------------------------
I: 407 (12.04%)
X: 282 (8.34%)
S: 280 (8.28%)
R: 249 (7.37%)
M: 247 (7.31%)
E: 243 (7.19%)
W: 223 (6.60%)
L: 209 (6.18%)
V: 197 (5.83%)
H: 120 (3.55%)
P: 120 (3.55%)
Q: 120 (3.55%)
Y: 119 (3.52%)
C: 110 (3.25%)
J: 85 (2.51%)
A: 78 (2.31%)
K: 71 (2.10%)
G: 61 (1.80%)
F: 52 (1.54%)
Z: 37 (1.09%)
T: 28 (0.83%)
O: 25 (0.74%)
B: 6 (0.18%)
D: 6 (0.18%)
N: 3 (0.09%)
U: 2 (0.06%)

┌──(kaliuser1㉿kaliuser)-[~/Documents]
└─$
```

Fig: Frequency of letter from task5_1.c using ciphertext.txt

Letter mappings:

A W

B X

C Y

D Z

E A

F B

G C

H D

I E

J F

K G

L H

M I

N J

O K

P L

Q M

R N

S O

T P

U Q

V R

W S

X T

Y U

Z V

Question 5-B

The key issue in the frequency analysis exercise was properly mapping ciphertext characters to their English equivalents based only on frequency. During the analysis, finding appropriate letter mappings based only on frequency was one of the biggest challenges. The frequency analysis wasn't always accurate because of the substitution cipher, but it was a good place to start. Additionally, it required several repetitions of rerunning the decryption and editing the mappings.txt in order to provide comprehensible data.

An important factor in the analysis's efficacy was the ciphertext's length. It offered a more trustworthy sample for frequency comparison due to its relative length. This procedure would have been considerably more difficult with a shorter ciphertext since the frequency of letters would not have been statistically significant, which would have decreased the analysis's accuracy. We employed several approaches to increase accuracy. The length of the cipher text undoubtedly had an impact on the technique. The longer excerpt was very beneficial in this case since it gave a more accurate letter distribution of frequency and made it easier to compare with standard English letter frequencies. A substantially shorter cipher text would have added additional noise and complicated the process of deriving trustworthy inferences from the range of data.

A significant approach was to use the frequency analysis output as a first-pass estimate by directly comparing it with known English letter frequencies. Following the emergence of incomplete words or sentence structures in the decrypted output, contextual signals and well-known literary terms assisted in validating or improving such estimates.

References

Adleman, L. M., Shamir, A. & Rivest, R. L., 2021. 45 A Method for Obtaining Digital Signatures and Public-Key Cryptosystems (1978). In: H. R. Lewis, ed. *Ideas That Created the Future: Classic Papers of Computer Science*. s.l.:MIT Press, pp. 463-474.

Vollala, S., Tiwari, U. & Ramasubramanian, N., 2021. Bit Forwarding Techniques for Efficient Modular Exponentiation. In: *Energy-Efficient Modular Exponential Techniques for Public-Key Cryptography*. s.l.:Springer, pp. 185-206.