CM2025: Computer Security

Midterm Assignment Part 2

Arjun Muralidharan

4th July 2021

Contents

1 Search the internet and learn about the Trifid Cypher

1.1 Make the appropriate grids using the key phrase

The 3×3 grids using the phrase "Baseball is my favourite sport" are shown below. These are constructed by filling in the grids with the unique letters of the key, and completing the grids with the rest of the alphabet.

Table 1. *Encryption Grids for Key Phrase*

	Layer 1				*Layer 2*				*Layer 1*		
	1	**2**	**3**		**1**	**2**	**3**		**1**	**2**	**3**
1	B	A	S	**1**	V	O	U	**1**	H	J	K
2	E	L	I	**2**	R	T	P	**2**	N	Q	W
3	M	Y	F	**3**	C	D	G	**3**	X	Z	+

1.1.1 Encrypt your name using those grid and block size 5. Show your work

Using the previous grids, the encryption is done by assembling the trigrams accordingly.

Table 2. *Trigrams based on encryption tables*

	A	*R*	*J*	*U*	*N*
Layer	**1**	**2**	**3**	2	3
Row	1	**2**	**1**	**1**	2
Column	2	1	**2**	**3**	**1**

The new trigrams are read horizontally (and bolded in the table), resulting in the encrypted ciphertext

`ICVRC`

1.2 Decrypt the string: RLQREERRLVVTV

This time, we apply the process in reverse by inserting the trigrams horizontally instead of vertically, and then reading them vertically to arrive at the plaintext.

Table 3. *Decrypted Message*

R	*L*	*Q*	*R*	*E*	*E*	*R*	*R*	*L*	*V*	*V*	*T*	*V*
2	2	1	1	2	2	3	2	2	2	2	1	1
2	1	1	2	1	2	2	1	2	2	1	1	2
2	2	1	1	2	1	1	2	2	2	2	1	1
T	**O**	**B**	**E**	**O**	**R**	**N**	**O**	**T**	**T**	**O**	**B**	**E**

2 We wish to use the RSA to encode the message: 20.

2.1 Explain why N cannot be $3 \cdot 7$

If $N = 3 \cdot 7 = 21$, then

$$\begin{aligned}
\Phi(21) &= \Phi(3) \cdot \Phi(7) \\
\Phi(21) &= (3-1) \cdot (7-1) \\
\Phi(21) &= 2 \cdot 6 \\
\Phi(N) &= \Phi(21) && = 12 \\
\Phi(p) &= (p-1) \qquad \text{if p is prime}
\end{aligned}$$

We now need e and d as keys. In order to get e, it holds that

1. e must be prime
2. $1 < e < \Phi(N)$
3. e is co-prime with N and $\Phi(N)$

Therefore, $e \in 5, 7, 11$.

We then need to find a number where d is the modular inverse of $e \bmod \Phi(N)$. The inverses of the candidates $5, 7$ and 11 are identical, i.e. they are also $5, 7, 11$. Therefore, this is not suitable for encryption as the public keys cannot be published without compromising security. Of course, they are also small enough and therefore easy to brute force.

2.2 Let N be $5 \cdot 7$, compute $\Phi(N)$

If $N = 5 \cdot 7 = 35$, then we know, based on Euler's totient function, that

$$gcd(N, k) = 1 \qquad \text{for } 1 \leq k \leq N$$

Since $35 = 5 \cdot 7$,

$$\begin{aligned}
\Phi(35) &= \Phi(5) \cdot \Phi(7) \\
\Phi(35) &= (5-1) \cdot (7-1) \\
\Phi(p) &= (p-1) \\
\Phi(35) &= 4 \cdot 6 \\
\Phi(N) &= \Phi(35) = 24
\end{aligned}$$

2.3 Compute an approximate value for e. Explain the answer.

e must be co-prime to $\Phi(N)$. We can pick 13 as e, $gcd(13, 24) = 1$ so it is suitable as e in a public key-pair.

2.4 Compute an approximate value for d. Explain the answer.

d will be part of the private key, to ensure that decryption happens correctly we need to ensure that $e \cdot d = 1 \bmod \Phi(N)$

Let's take $e = 37$ as $37 \cdot 13 = 481$ and $481 = 1 \bmod 24$ (calculated by trying all values up to 37).

2.5 Encode the message "20". Explain your answer.

We can encrypt the message like so:

$$E = M^e \bmod N$$
$$E = 20^{13} \bmod 35$$
$$E = 20$$

Here, the cipher matches the plaintext exactly. However, with long enough prime numbers, this is unlikely to apply in a real scenario.

2.6 Decode the encoded message. Explain your answer.

The same process can be used to decode the message.

$$M = E^d \bmod N$$
$$M = 20^{37} \bmod 35$$
$$M = 20$$

Again, the plaintext matches the cipher.