Homework 4

Blake Moore

1.1. Packet 1: Source: 192.168.1.126 Destination: 131.204.138.170
Packet 2: Source: 131.204.138.170 Destination: 192.168.1.126

1.2. Packet 1: Source: bc:83:85:d2:b1:da Destination: 4c:ab:f8:03:cc:49
Packet 2: Source: 4c:ab:f8:03:cc:49 Destination: bc:83:85:d2:b1:da

1.3. Packet 1: Length: 20 bytes Protocol: TCP(6) TTL: 128
Packet 2: Length: 20 bytes Protocol: TCP(6) TTL: 237

1.4. Packet 1: Source: 57654 Destination: 80
Packet 2: Source: 80 Destination: 57654

1.5. Packet 1: Length: 954 Raw: 1205065333
Packet 2: Length: 123 Raw: 2641346977

1.6. Connection type, browser type, OS type and version, encoding type, Language, saved cookies

1.7. Source: 192.168.1.126, Destination: 142.251.15.138

1.8. 60 bytes ← total length (20 bytes for header)

1.9. ICMP(1)

1.10. Type: 8 (Echo (ping) request) Code: 0

1.11. Type: 0 (Echo (ping) reply) Code: 0

2. Confidentiality, Integrity, and Availability
Confidentiality: The practice of keeping private information and resources private. This means keeping private matrials encrypted or hidden in a way that only those who should access it can.
Integrity: Protection of data from unauthorized change. Also the assured identification of the data.
Availability: Making resources and information available and accessible to users.

3. helpme = 42, 27, 62, 82, 63, 27 $\xrightarrow{\text{mod } 26}$ 16, 1, 10, 4, 15, 1 = qbkepb
7, 4, 11, 15, 13, 4

4. vmvrz = xiqv
$c = 11x + 2 \bmod 26$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
o	h	q	t	m	f	y	r	k	d	w	p	i	b	u	n	g	z	s	l	e	x	q	j	c	v

5.A. $17^{-1} \bmod 101 = 6$

A.

i	r_i	u_i	v_i	q_i
1	101	1	0	
2	17	0	1	5
3	16	1	-5	1
4	1	-1	6	16

B.

i	r_i	u_i	v_i	q_i
1	1234	1	0	
2	357	0	1	3
3	163	1	-3	2
4	-31	-2	7	5
5	8	11	-38	3
6	7	-35	121	1
7	1	46	-159	

B. $355^{-1} \bmod 1234 = 1234 - 159 = 1075$

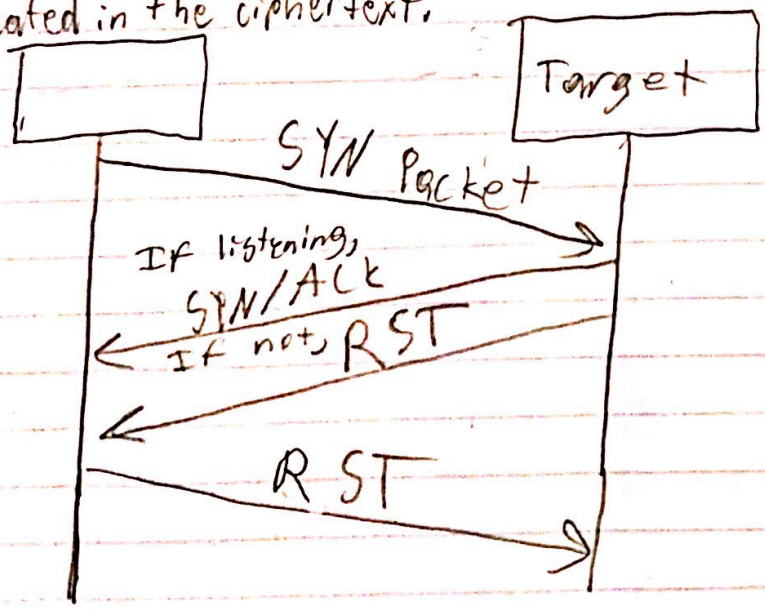
C. $3125^{-1} \bmod 9987 = 1844$

i	r_i	u_i	v_i	q_i
1	9987	1	0	
2	3125	0	1	3
3	612	1	-3	5
4	65	-5	16	9
5	27	46	-147	2
6	11	-97	310	2
7	5	240	-767	2
8	1	-577	1844	

6. Trials and code submitted separately . . . . . .
Correct one:
Shift/cipher key: 16
Decrypted: LOOKUPINTHEAIRITSABIRDITSAPLANEITSSUPERMAN

7. ECB: A simple block cipher mode that divides plaintext into fixed-size and encrypted 'blocks' using the same key.
CBC: A block cipher mode where plaintext is divided into blocks and XORed with the previous ciphertext block.
ECB is not a good mode for encrypting a sequence of blocks because it is less secure due to plaintext patterns being repeated in the ciphertext.

8.



9. C

10. A

11. E