COMP 3334 Assignment 1

JAHJA Darwin, 16094501d

Let my X = 16094501

Q1

Given plaintext: `WELCOMETOTHEBIGSCREENS`

The Secret Key is: $(16094501)^{10}$ mod $26 = 17$

Then, the plain to cipher mapping is:

```
Plain:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: RSTUVWXYZABCDEFGHIJKLMNOPQ
```

Therefore, the encrypted cipher text is `NVCTFDVKFKYVSZXJTIVVEJ`.

Q2

Given Integer $X = 16094501$; Modulo $M = 26$.

If $gcd(X, M) = 1$, then the multiplicative inverse X^{-1} exists. Here, $gcd(16094501, 26) = 1$. Therefore, in this case, X^{-1} exists.

To find X^{-1}, we can use **Extended Euclidean Algorithm**:

Steps:

A1	A2	A3	B1	B2	B3	T1	T2	T3	Q
1	0	26	0	1	16094501	1	0	26	0
0	1	16094501	1	0	26	-619019	1	7	619019
1	0	26	-619019	1	7	1857058	-3	5	3
-619019	1	7	1857058	-3	5	-2476077	4	2	1
1857058	-3	5	-2476077	4	2	6809212	-11	1	2
-2476077	4	2	6809212	**-11**	**1**				

Therefore, the modular multiplicative inverse of 16094501 is -11 mod $26 = 15$

Q3

The 5x5 matrix using key `MANGKHUT`:

M	A	N	G	K
H	U	T	B	C
D	E	F	I/J	L
O	P	Q	R	S
V	W	X	Y	Z

Cipher text decrypting:

```
Cipher:    AP SL VH FU QH UD IR KR BS FW FA QZ
Decrypted: WE LC OM ET OT HE BI GS CR EX EN SX
```

Therefore, the original message is `WELCOMETOTHEBIGSCREENS`.

Q4

DES has a key size of 56-bit. Thus, there are 2^{56} possible key combinations. Assuming that cracking a DES takes 0.5 hour, thus, the amount of time for the system to try each key is $0.5/2^{56}$ hour.

Also, we assume that the time to try out each DES key is equal to that for each AES key. As AES-128 has a key size of 128-bit, so it has 2^{128} possible key combinations. Therefore, the time to break AES-128 is:

$$2^{128} \cdot (0.5/2^{56}) = 2^{71} \text{ hour}$$

Taking 1 mean year as 8765.82 hours, and the age of the Earth as 4.54×10^9 years:

$$(2^{71}/8765.82)/4.54 \times 10^9 = 5.933 \times 10^7 \text{ age of Earth}$$

Therefore, the time in terms of the Age of the Earth to break AES-128 is 5.933×10^7.

Q5

Given $n = 16109$ and $e = 97$. As $pq = n$, the prime numbers p and q can be obtained by factorization: $p = 181, q = 89$. Then, $\psi(n) = 180 \cdot 88 = 15840$.

$e \cdot d = 1 \ mod \ \psi(n) \rightarrow 97 \cdot d = 1 \ mod \ 15840$, To obtain d, we can use **Extended Euclidean Algorithm**.

Steps:

A1	A2	A3	B1	B2	B3	T1	T2	T3	Q
1	0	15840	0	1	97	1	-163	29	163
0	1	97	1	-163	29	-3	490	10	3
1	-163	29	-3	490	10	7	-1143	9	2
-3	490	10	7	-1143	9	-10	1633	1	1
7	-1143	9	-10	**1633**	**1**				

Therefore, $d = 5$ and plaintext $M = C^d \ mod \ n = (2018)^5 \ mod \ 16109 = 1037$.

Q6

A secure online voting system needs to meet the following security requirement:

1. Secure connections

The system needs to ensure that the communication tunnel between the voter and the system is secure. This can be done by using HTTPS which encrypts the communication between two ends using TLS. Also, the system can generate unique links for each active session to prevent the link being reused or duplicated by others.

2. Secure Authentication

Authenticating remote user is one of the biggest difficulties as we need to ensure the real identity of the voter. In order to secure the authentication process, the system can adopt the 2-way authentication method which generates an one-time password at real time and sent to the voters through short message service when the voter login to the system. This can prevent the voter's identity accessed by other people.

3. Anonymity

The system needs to ensure the anonymity of the voting data, which all completed ballots inside the ballot box do not contain voters' identity information. This can protect the voter's privacy and prevent the ballot's identity retrieved by other people.

4. Uniqueness

The system should ensure that all voters can only vote once. To achieve this, the system can generate unique token for each voter and the token will be discard after the voter completes one successful ballot.

5. Protecting critical infrastructure (The ballot box)

The system should have a secure infrastructure which isolates the ballot box to the public as well as decentralizing the election process to multiple sub-systems, which only handle part of the election data to reduce the risk of data loss. Also, the system should have defensive mechanisms against various attacks such as Denial-of-service attacks to ensure the stability of the system.

Q7 1.

The system implements a three-domain model to secure the Payment Authentication in the online transaction process, which the customers can direct interact with the card issuing bank without letting the merchant knowing the detail of the card. It requires the customer to enter the a special security code generated by the card issuer to verify the legitimate owner of the card.

Q7 2.

The seller in the 3D-secure does not hold the digital certificate for the payment authentication process. Instead, it only holds the token for the authorization of the payment process sent by the banking card issuer.