Assignment-I

Question 1:

Concurring to the secure communication framework, we never utilize encryption/decryption calculations since programmers can hack them and the communication isn't ensured that it cannot be tuned in to by third parties, so we never utilize them. There are various negatives to algorithms because in the event that there's a consistent blunder, the whole communication can be disrupted. Now, when we communicate utilizing encryption/decryption keys, all we have maybe a open key and a private key. Let me go over the distinction between a private key and a open key. Let's take a see at an illustration where A and B are communicating whereas the others are endeavoring to unscramble and scramble the information to avoid it from unauthorized getting to or utilization. It's on the off chance that they can't communicate since they do not have to get to. Presently, let's the conversation around the private key, which is utilized when decoding is done with a fair get-to. As a result, when compared to encryption/decryption calculations, the decoding and encryption key is the foremost vital.

Challenges that we need to face while using Algorithms instead of Keys:

Designing a secure encryption/decryption algorithm is awfully hard. The only approved method which offers some considerable reliability is the designing of an algorithm to make it public. Let allow the algorithm available to all public platforms for cryptographers who are looking to break the flaws in the system. If, after a couple of decades none of them break the flaws in the algorithm, then it is probably not too weak. With a secret algorithm, you have to do all the testing, and cross verification on your own, which is not acceptable in any finite amount of time.

A secret algorithm still available as source code on some computer, transformed in to binaries using compilers on some others, and carried by lead of designer. Unless all the involved algorithm implemented systems and the designer's database were dissolved, it is very hard to prevent that "secret algorithm" from leaking everywhere. On the other hand, a secret key is a small element that can be more efficiently and effectively managed and kept secret since it was stored in the RAM.

Question 2.a

(2)(i) Euler's theorem: Let $a \in \mathbb{Z}$, and $m \in \mathbb{Z}^+$.
If $(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \bmod m$

(ii) Fermat's Little theorem is thus a specific case of Euler's theorem. where $m = p$ and p is prime number since $\varphi(p) = p - 1$.

(iii) Euler phi-function is defined by

$$\varphi(n) = |\{x \in \mathbb{Z} : 1 \le x \le n;\ (x, n) = 1\}|$$

where $n \in \mathbb{Z}^+$. In otherwords, $\varphi(n)$ is the no. of positive integers less than or equal to n that are relatively prime to 'n'.

(a) Compute $7^{97} \bmod 13$ (or) $7^{97} \equiv x \bmod 13$

$\varphi(13) = |\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}| = 12$ [∵ (ii)]

since $(97, 13) = 1$ [∵ (iii)]

By Euler's theorm $7^{\varphi(13)} \equiv 1 \bmod 13$ [∵ (i)]

$7^{12} \equiv 1 \bmod 13$

Hence $7^{97} \bmod 13 = (1)^8 \cdot 7^1 \bmod 13$

$= 7 \bmod 13 = \underline{\underline{7}}$

So $\boxed{x = 7}$

Question 2.b

(b) Compute 3^{302} mod 13 (or) $3^{302} \equiv x$ mod 13

$\phi(13) = |\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}| = 12$ [∵ (ii)]

since $(302, 13) = 1$ [∵ (iii)]

By Euler's theorem, $3^{\phi(13)} \equiv 1$ mod 13

$3^{12} = 1$ mod 13 [∵ (i)]

Hence 3^{302} mod 13 $\equiv (3^{12})^{25}$ mod 13 . 3^{2} mod 13

$\equiv$ 1 . 9 . mod 13

3^{302} mod 13 $\equiv$ 9 mod 13

$=$ 9.

∴ $\boxed{x = 9}$

Question 3.a:

It is characterized as an Progress Encryption standard in which the same key is utilized to scramble and translate information. It scrambles utilizing the substitution stage arrange calculation and a few rounds. It is based on a substitution-permutation network, also known as an SP network. It consists of a series of linked operations, including replacing inputs with specific outputs (substitutions) and others involving bit shuffling (permutations). The AES encryption keys are accessible in three lengths. Each key incorporates an interesting set of key combinations. Such as 128-bit, 192-bit, and 256-bit, It is presently one of the most noteworthy encryption conventions accessible, with the finest security and speed. The lengths of the keys exponentially increase the difficulty of deciphering the code. AES became the standard in 2002, and the NIST reevaluates it every five years in an effort to find flaws and make improvements. It is ideal to utilize the industry standard for encryption. The calculation for key extension: The AES Key extension is nothing, but the calculation acknowledges a four-word (16byte) key as input and the strategy could be a straight cluster of 44 words (176 bytes). The key is duplicated into four bigger keywords. The rest of the amplified key is completed four words at a time. Each modern word w[] is subordinate to the word promptly going before it, w[i-1], and the word four positions back, w[i-4]. A basic XOR is utilized. In this calculation, more advanced work is utilized for a word whose position in the w array is a multiple of 4.

Cases of the AES Encryption with few examples:

1) VPN (Virtual private networks) 2) Wi-fi 3) Versatile applications 4) OS framework components. 5) Programming dialect libraries. 6) Watchword managers.

Question 3.b:

AES	DES	3DES
AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard	3DES stands for Triple Data Encryption Standard
AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities	3 DES is a variation of DES which is secure than the usual DES.
AES is created by Vincent Rijmen and Joan Daemen.	DES is created by IBM	3DES is also created by IBM.
The block size of AES is 128 bits.	It is very slower than AES. DES has a block size of 64 bits.	3DES has a block size of 64 bits.
key length of AES is 128, 192, and 265 bits..	DES is created by IBM. Its key length is 56 bits.	3DES is also created by IBM. key length of 3DES is 168,112 bits.
AES works very fast, faster than 3DES.	It is very slower than AES.	3DES is very slower than AES.

Question 4.a:

(4) Multiplicative inverse of 5 in Z_{12} ?

It means 5^{-1}. mod 12.

We want 'v' such that $5v = 1 - 12w$

$5v \equiv 1 \cdot \text{mod } 12.$

Euclid's Algorithm:

$12 = 5 \cdot (2) + 2$ $\quad [\because n = q \cdot m + r]$

$5 = 2(2) + 1$

Rewritten as, $5 + 2(-2) = 1$ —— (1)

$12 + 5(-2) = 2$ ⟶ (2)

Substitute (2) in (1)

$5 + [12 + 5(-2)](-2) = 1$

$5 + 12(-2) + 5(4) = 1$

$5(5) + 12(-2) = 1$

$5(\underset{v}{5}) = 1 + 12(2) = 1 - 12(\overset{w}{-2})$

$\equiv 1 (\text{mod } 12)$ $\quad v = 5, \; w = -1$

Hence '5' is multiplicative inverse of 5 (mod 12)

i.e. $\boxed{5^{-1} \cdot (\text{mod } 12) = 5}$

Question 5.a:

5(a) $19x = 1 \mod 77.$

Solve this problem using Multiplicative inverse of $19 \pmod{77}$.

using Euclid's theorm

$$m = q * n + r = n * q + r$$

$$77 = 19 * 4 + 1 \quad [\because \gcd(19, 77) = 1]$$

$$77 + 19(-4) = 1$$

$19v \equiv 1 \mod 77$

$19v + 77w = 1.$

$x = 19 \cdot v \cdot \mod(77)$

$$\overset{0}{\cancel{77}} + 19(-4) = 1 \mod 77$$

$$19(73) = 1 \mod 77.$$

$$\therefore \quad 19x \equiv 1 \mod 77$$

$$73 * 19x = 1 * 73 \mod 77$$

$$x \equiv 73 \mod 77.$$

check: $19x \equiv 1 \pmod{77}$

$$19 \cdot (73 \mod 77) \equiv 1 \pmod{77}$$

$$1387 \mod 77 \equiv 1 \pmod{77}$$

$$1 \mod 77 \equiv 1 \pmod{77}$$

$$[\because 1387 = 77 * 18 + 1]$$

Question 5.b:

5(b) Multiplicative inverse of 19. mod 77.

(or) $19x \equiv 1 \cdot \bmod 77$. using Extended Euclidian Algo.

Q	A	B	R	T_1	T_2	T
4	77	19	1	0	1	-4
19	19	1.	0	1	-4	77
X	1	0	X	$\boxed{-4}$	77	X ← STOP.

↑ Answer

Multiplicative Inverse of 19 mod 77 i.e

$19x \equiv 1 \cdot \bmod 77$

$19 \cdot (-4) \equiv 1 \cdot \bmod 77$

$19(73) \equiv 1 \cdot \bmod 77.$

$\therefore$ $19x \equiv 1 \cdot \bmod 77$

$73^* \, 19x \equiv 73^* \bmod 77$

$x \equiv 73 \bmod 77.$

check: $19x \equiv 1 \cdot (\bmod 77)$

$19(73 \bmod 77) \equiv 1 \cdot (\bmod 77)$

$1387 \bmod 77 \equiv 1 \cdot \bmod 77$

$1 \bmod 77 \equiv 1 \cdot \bmod 77$

$[\because 1387 = 77 * 18 + 1]$

Question 5.c:

5(c) $19x \equiv 30 \mod 77$.

We want to workout a multiplicative inverse of 19 (mod 77) i.e. 19^{-1}. (mod 77)

$77 = 19 * 4 + 1$ (∵ gcd(19, 77) = 1)

$\overset{0}{\cancel{77}} + 19(-4) = 1$. [∵ divisible by 77]

$\boxed{19(73) \equiv 1 \pmod{77}}$

19 v = 1.(mod 77)

19v + 77 w = 1

x ≡ 19 v.(mod 7

∴ $19x \equiv 30 \mod 77$

$19 \times 73x \equiv 30 * 73 \mod 77$

$\boxed{x \equiv 34 \mod 77}$

Check:– $19 \cdot x = 30 \mod 77$

$19 \cdot (34 \mod 77) \equiv 30 \cdot \mod 77$

$646 \mod 77 \equiv 30 \mod 77$

$\boxed{30 \mod 77 \equiv 30 \mod 77}$

Since (∵ $646 = 77 * 8 + 30$)