ASSIGNMENT

CSPC 631 Principles of Cryptography

Name :- Amit Kumar
Branch/Sec. :- CSE/"B"
Roll No. :- 10612101 2

ASSIGNMENT

CSPC63| Principles of Cryptography. ROLL NO.:- 106121012

1) Ans:-

Cryptanalytic Attack on AES.

The Advance Encryption standard (AES) is a robust encryption algorithm widely employed for data security.

Two main Approaches to cryptanalyzing AES are:-

1.) Differential cryptanalysis:

- This technique exploits weakness statical weakness in how the algorithm handles differences within the original massage (plain Text).
- Attackers introduce, controlled change to the plain Text and observe the resulting behaviour/ Variation in the Cipher Text. By Analysing these changes, they might theoretically recover the secret key.
- AES's design specifically counters differential cryptanalysis. The number of encryption round is choosen to make such attacks computationally infeasible.

2) Linear cryptanalysis

- This method search for linear relationships between key, plain Text and Cipher text.
- Attackers Construct a series of equations that exploits these relationships to gain information about the key. These equations relate specific bits in the plain text and key to specific bits in the Cipher Text.

Hence, cryptanalysis plays a vital role in ensuring the continued security of encryption standards. while both differential and linear cryptanalysis pose theoretical threats, AES's design effectively mitigates these risks.

ROLL NO.:- 106121012

Q.no.2.) Calculate Jacobi symbol $\left(\frac{a}{b}\right) = ?$

i) $\left(\frac{11}{15}\right)$

$15 \rightarrow 3 \times 5$

$$\left(\frac{11}{15}\right) = \left(\frac{11}{3\times5}\right) = \left(\frac{11}{3}\right)\left(\frac{11}{5}\right)$$

#note:-

- $a \equiv b \pmod p$
- $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right)$
- $\left(\frac{a}{p}\right) = a^{\left(\frac{p-1}{2}\right)} \pmod p$

For, $\left(\frac{11}{3}\right)$:

$11 \bmod 3 = 2 \bmod 3$

$\therefore 11 \equiv 2 \bmod 3$

so, $\left(\frac{11}{3}\right) \equiv \left(\frac{2}{3}\right)$

$= 2^{\left(\frac{3-1}{2}\right)} \bmod 3$

$= 2 \bmod 3 \equiv -1 \pmod 3$

$\therefore \left(\frac{11}{3}\right) = -1$

For $\left(\frac{11}{5}\right)$:

$11 \bmod 5 \equiv 1 \bmod 5$

$11 \equiv 1 \bmod 5$

$\therefore \left(\frac{11}{5}\right) \equiv \left(\frac{1}{5}\right) = 1^{\left(\frac{5-1}{2}\right)} \pmod 5 = 1 \pmod 5 = 1$

$\therefore \left(\frac{11}{5}\right) = 1$

But,

$\left(\frac{11}{15}\right) = \left(\frac{11}{3}\right) \cdot \left(\frac{11}{5}\right)$

put the valve of $\left(\frac{11}{3}\right)$ and $\left(\frac{11}{5}\right)$,

$\left(\frac{11}{15}\right) = -1 * 1 = -1$.

$\therefore \boxed{\left(\frac{11}{15}\right) = -1}$

ii.) $\left(\frac{13}{21}\right)$

$$\left(\frac{13}{21}\right) = \left(\frac{13}{3\times7}\right) = \left(\frac{13}{3}\right)\cdot\left(\frac{13}{7}\right)$$

Performing calculation for $\left(\frac{13}{3}\right)$:

$13 \pmod 3 \equiv 1 \pmod 3$

$13^{\left(\frac{3-1}{2}\right)} \equiv 1 \bmod 3$

$\therefore \left(\frac{13}{3}\right) \equiv \left(\frac{1}{3}\right) \equiv 1 \bmod 3 \equiv 1 \bmod 3$

$\therefore \boxed{\left(\frac{13}{3}\right) = 1}$ —— (1)

Now, Performing calculation For $\left(\frac{13}{7}\right)$:

$13 \pmod 7 = 6 \pmod 7$

$13 \equiv 6 \pmod 7$

$\therefore \left(\frac{13}{7}\right) \equiv \left(\frac{6}{7}\right) = 6^{\left(\frac{7-1}{2}\right)} \bmod 7 = 6^3 \bmod 7$

$= -1$

$\therefore \boxed{\left(\frac{13}{7}\right) = -1}$ —— (II)

But, $\left(\frac{13}{21}\right) = \left(\frac{13}{3}\right)\cdot\left(\frac{13}{7}\right)$

$\therefore$ from eq—(1) and (2),

$\left(\frac{13}{21}\right) = 1 * -1 = -1$

$\therefore \boxed{\left(\frac{13}{21}\right) = -1}$

---

iii.) $\left(\frac{11}{35}\right)$

$$\left(\frac{11}{35}\right) = \left(\frac{11}{5\times7}\right) = \left(\frac{11}{5}\cdot\right)\left(\frac{11}{7}\right)$$

now performing calculation for $\left(\frac{11}{5}\right)$:

$11 \pmod 5 \equiv 1 \pmod 5$

$11 \equiv 1 \pmod 5$

$\therefore \left(\frac{11}{5}\right) \equiv \left(\frac{1}{5}\right) \equiv 1^{\left(\frac{5-1}{2}\right)} \bmod 5 = 1$

$\therefore \boxed{\left(\frac{11}{5}\right) = 1}$ —— (1)

CSPC631 Principles of Cryptography ASSIGNMENT

Roll No:- 10612101 2 (5)

now, Performing calculation for $(\frac{11}{7})$:

$11 \pmod 7 \equiv 4 \pmod 7$

$11 \equiv 4 \pmod 7$

$\therefore \left(\frac{11}{7}\right) \equiv \left(\frac{4}{7}\right) \equiv \left(\frac{2^2}{7}\right) = 1$

$\therefore \boxed{\left(\frac{11}{7}\right) = 1}$ — (ii)

note:-

$\left(\frac{a^2}{p}\right) = 1$

Now,

$\left(\frac{11}{35}\right) = \left(\frac{11}{5}\right) \cdot \left(\frac{11}{7}\right)$

From eq-(i) and (ii), we get

$\left(\frac{11}{35}\right) = 1 * 1 = 1.$

$\therefore \boxed{\left(\frac{11}{35}\right) = 1}$

---

iv.) $\left(\frac{2}{75}\right)$

$\left(\frac{2}{75}\right) = \left(\frac{2}{3 \cdot 5 \cdot 5}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) \cdot \left(\frac{2}{5}\right)$

Performing calculation for: $\left(\frac{2}{3}\right)$

$\left(\frac{2}{3}\right) \equiv 2^{\left(\frac{3-1}{2}\right)} \bmod 3 = 2 \pmod 3 = -1$

$\therefore \boxed{\left(\frac{2}{3}\right) = -1}$ — (i)

now,

Performing calculation for $\left(\frac{2}{5}\right)$

$\therefore \left(\frac{2}{5}\right) = 2^{\left(\frac{5-1}{2}\right)} = 2^2 \bmod 5 = 4 \pmod 5 = -1$

$\therefore \boxed{\left(\frac{2}{5}\right) = -1}$ — (ii)

now, $\left(\frac{2}{75}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) \cdot \left(\frac{2}{5}\right)$

From eq-(i) and (ii), we get

$\left(\frac{2}{75}\right) = -1 * -1 * -1 = -1$

Hence, $\boxed{\left(\frac{2}{75}\right) = -1}$

v.) $\left(\frac{5}{21}\right)$

$\therefore \left(\frac{5}{21}\right) = \left(\frac{5}{3\times7}\right) = \left(\frac{5}{3}\right)\cdot\left(\frac{5}{7}\right)$

Performing calculation for, $\left(\frac{5}{3}\right)$

$5 \pmod 3 \equiv 2 \pmod 3$

$5 \equiv 2 \pmod 3$

$\therefore \left(\frac{5}{3}\right) \equiv \left(\frac{2}{3}\right) \equiv 2^{\left(\frac{3-1}{2}\right)} \pmod 3$

$= 2 \pmod 3 = -1 \pmod 3 = -1$

$\therefore \boxed{\left(\frac{5}{3}\right) = -1}$ —— (i)

Performing calculation for, $\left(\frac{5}{7}\right)$

$\left(\frac{5}{7}\right) = 5^{\left(\frac{7-1}{2}\right)} \pmod 7$

$= 5^3 \pmod 7$

$= 125 \pmod 7$

$= -1 \bmod 7 = -1$

$\therefore \boxed{\left(\frac{5}{7}\right) = -1}$ —— (ii)

Now, $\left(\frac{5}{21}\right) = \left(\frac{5}{3}\right)\left(\frac{5}{7}\right)$

From equation (i) and (ii), we get

$\left(\frac{5}{21}\right) = -1 * -1 = -1$

$\therefore \boxed{\left(\frac{5}{21}\right) = -1}$