USN										

CELEBRATING 25 YEARS
CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A+ GRADE BY NAAC

INTERNAL ASSESSMENT TEST – I

Sub:	CRYPTOGRAPHY							Code:	18EC744
Date:	21/ 10 / 2022	Duration:	90 mins	Max Marks:	50	Sem:	VII	Branch:	ECE

Answer any 5 full questions

		Marks	CO	RBT
1	Explain the types of cryptanalytic attacks on encrypted messages.	[10]	CO1	L1
2	Encrypt the message “work is worship” using, play fair cipher with the keyword “COMPUTER” and decrypt the cipher text to recover the original message. Give the rules for encryption and decryption.	[10]	CO1	L3
3	Encrypt the plain text “monday” using Hill cipher with key =$\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}$. Show your calculations to obtain cipher text. (Use a =0, b=1 …z=25).	[10]	CO1	L3

4	Define the modular arithmetic operation with necessary properties and prove the same.	[10]	CO5	L1
5	a. Apply the procedure to calculate the GCD using Euclidean algorithm and determine the GCD of (1160718174, 316258250). b. Distinguish between block cipher and stream cipher with examples.	[5] [5]	CO3 CO1	L3 L1
6	a. What are groups? Explain in detail with respect to its properties a. Prove that if a×c ≡b×c (mod n) then a ≡ b (mod n) if c is relatively prime to n.	[5] [5]	CO4 CO3	L1 L3
7	a. Develop a set of additive and multiplicative tables for modulo-8. b. Using extended Euclidean algorithm, find the multiplicative inverse of 550 (mod 1769).	[5] [5]	CO3 Co3	L2 L3

Scheme of solutions

Q. no.	Questions	Marks
1.	Explain the types of cryptanalytic attacks on encrypted messages.	10M

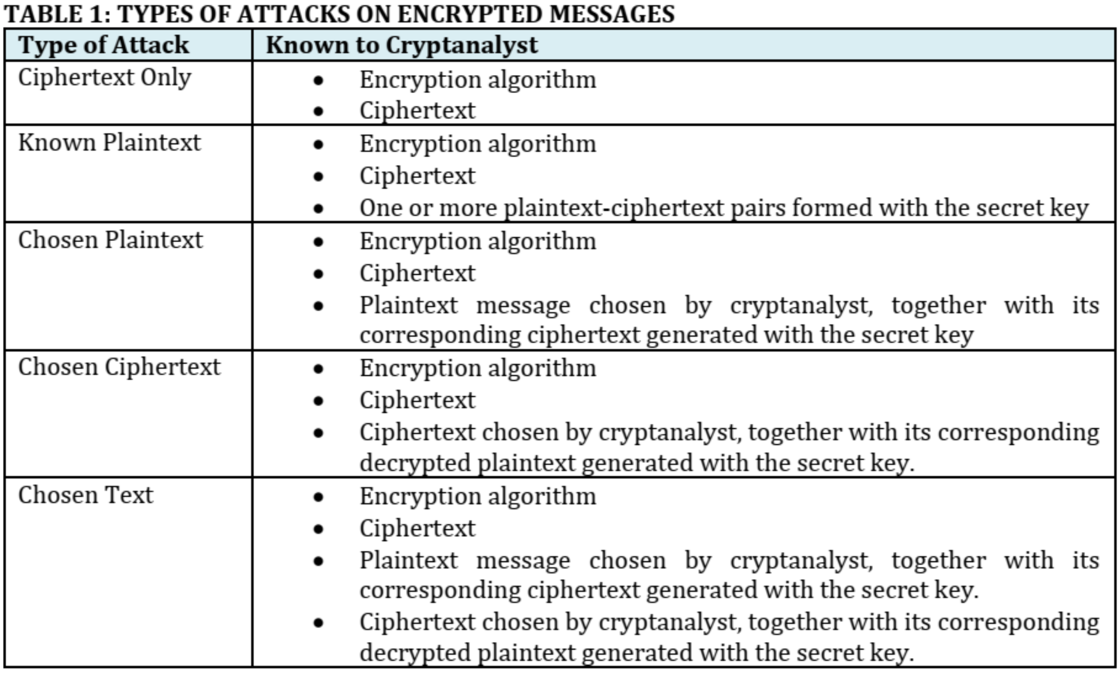


TABLE 1: TYPES OF ATTACKS ON ENCRYPTED MESSAGES

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key. • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

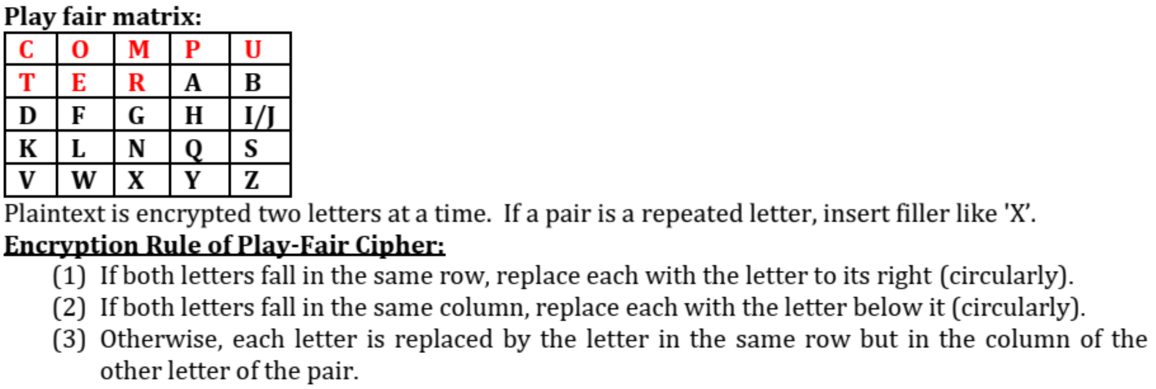
Cryptanalysis:

The whole point of cryptography is to keep the plain text secret from the eavesdropper. Cryptanalysis is the art or science of recovering the plain text without access to the key. Successful cryptanalysis may recover the plain text or the key. It also may find the weakness in a cryptosystem. An attempted cryptanalysis is called an attack. In real world cryptanalysts don't always have such detailed information. But it is assumed that the cryptanalyst has the knowledge of the encryption algorithm. There are several types of cryptanalytic attacks.

a) Cipher text only attack
b) Known Plain text attack
c) Chosen Plain text attack
d) Adaptive chosen Plain text attack
e) Chosen cipher text attack
f) Rubber-hose cryptanalysis

2. Encrypt the message "work is worship" using, play fair cipher with the keyword "COMPUTER" and decrypt the cipher text to recover the original message. Give the rules for encryption and decryption.

10M



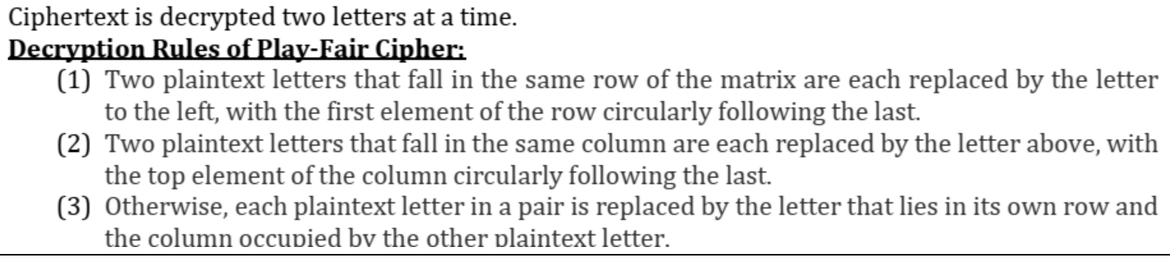
Play fair matrix:

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

Plaintext is encrypted two letters at a time. If a pair is a repeated letter, insert filler like 'X'.

Encryption Rule of Play-Fair Cipher:

(1) If both letters fall in the same row, replace each with the letter to its right (circularly).
(2) If both letters fall in the same column, replace each with the letter below it (circularly).
(3) Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair.



Ciphertext is decrypted two letters at a time.

Decryption Rules of Play-Fair Cipher:

(1) Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the left, with the first element of the row circularly following the last.
(2) Two plaintext letters that fall in the same column are each replaced by the letter above, with the top element of the column circularly following the last.
(3) Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied bv the other plaintext letter.

Encryption:

Plain Text	wo	rk	is	wo	rs	hi	px
Rule	2	3	2	2	3	1	3
Cipher Text	OE	TN	SZ	OE	BN	ID	MY

Decryption:

Cipher Text	OE	TN	SZ	OE	BN	ID	MY
Rule	2	3	2	2	3	1	3
Plain Text	wo	rk	is	wo	rs	hi	px

Plain Text: WO RK IS WO RS HI PX
Cipher Text: OE TN SZ OE BN ID MY

3. Encrypt the plain text “monday” using Hill cipher with key $=\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show your calculations to obtain cipher text. (Use a =0, b=1 …z=25).

10M

Divide the plain text into block of 2(as here key is a 2 × 2 matrix)

Plain Text: MO ND AY

$C = KP \, mod \, 26$

$$\begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \times \begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \end{bmatrix} \; mod \; 26$$

$$\begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} M & N & A \\ O & D & Y \end{bmatrix} mod26 = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 12 & 13 & 0 \\ 14 & 3 & 24 \end{bmatrix} mod26$$

$$\begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \end{bmatrix} = \begin{bmatrix} 164 & 129 & 96 \\ 158 & 86 & 168 \end{bmatrix} mod26 = \begin{bmatrix} 8 & 25 & 18 \\ 2 & 8 & 12 \end{bmatrix} mod26 = \begin{bmatrix} I & Z & S \\ C & I & M \end{bmatrix}$$

Cipher Text : ICZISM

4. Define the modular arithmetic operation with necessary properties and prove the same.

10M

Property	Expression
Commutative Laws	$(a + b) mod \, n = (b + a) \, mod \, n$ $(a \times b) mod \, n = (b \times a) \, mod \, n$
Associative Laws	$[(a + b) + c] mod \, n = [a + (b + c)] mod \, n$ $[(a \times b) \times c] mod \, n = [a \times (b \times c)] mod \, n$
Distributive Law	$[a \times (b + c)] mod \, n = [(a \times b) + (a \times c)] mod \, n$ $[a + (b \times c)] mod \, n = [(a + b) \times (a + c)] mod \, n$
Identities	$(0 + a) mod \, n = a \, mod \, n$ $(1 \times a) mod \, n = a \, mod \, n$
Inverse	$a + k = 0 \, mod \, n \quad where \; k = (-a)$ $a \times k = 1 \, mod \, n \quad where \; k = \; a^{-1}$

Let a = 1, b = 5, c = 3 and n = 8

Commutative Laws:

1. $(a + b) mod \, n = (1 + 5) mod \, 8 = 6 \quad (LHS)$
   $(b + a) \, mod \, n = (5 + 1) mod \, 8 = 6 \quad (RHS)$
   LHS = RHS (proved)
2. $(a \times b) mod \, n = (1 \times 5) mod \, 8 = 5 \quad (LHS)$
   $(b \times a) \, mod \, n = (5 \times 1) mod \, 8 = 5 \quad (RHS)$
   LHS = RHS (proved)

Associative Laws:

1. $[(a + b) + c] mod \, n = [(1 + 5) + 3] mod \, 8 = [6 \, mod \, 8 + 3 \, mod \, 8] mod \, 8 = [9] mod \, 8 = 1 \quad (LHS)$
   $[a + (b + c)] mod \, n = \; [1 + (5 + 3)] mod \, 8 = [1 \, mod \, 8 \; + 0 \, mod \, 8] mod \, 8 = [1] mod \, 8 = 1 \quad (RHS)$
   LHS = RHS (proved)
2. $[(a \times b) \times c] mod \, n = [(1 \times 5) \times 3] mod \, 8 = [5 \, mod \, 8 \; \times 3 \, mod \, 8 \,] mod \, 8 = [15 \,] mod \, 8 = 7 \quad (\, LHS)$
   $[a \times (b \times c)] mod \, n = [1 \times (5 \times 3)] mod \, 8 = [1 \, mod \, 8 \; \times 15 \, mod \, 8 \,] mod \, 8 = [7] mod \, 8 = 7 \quad (RHS)$
   LHS = RHS (proved)

Distributive Law:

1. $[a \times (b + c)] mod\ n = [1 \times (5 + 3)] mod\ 8 = [1\ mod\ 8 \times 8\ mod\ 8] = [0] mod\ 8 = 0\quad (LHS)$
   $[(a \times b) + (a \times c)] mod\ n = [(1 \times 5) + (1 \times 3)] mod\ 8 = [5 + 3] mod\ 8 = 0\quad (RHS)$
   LHS = RHS (proved)
2. $[a + (b \times c)] mod\ n = [1 + (5 \times 3)] mod\ 8 = [1\ mod\ 8\ + 15\ mod\ 8] = [1 + 7] mod\ 8 = 0\quad (LHS)$
   $[(a + b) \times (a + c)] mod\ n = [(1 + 5) \times (1 + 3)] mod\ 8 = [6\ mod\ 8 \times 4\ mod\ 8] = 24\ mod\ 8 = 0\quad (RHS)$

Identities:

1. $(0 + a) mod\ n = (0 + 1) mod\ 8 = 1$
2. $(1 \times a) mod\ n = (1 \times 1) mod\ 8 = 1$

Inverse:

1. $b + k = 0\ mod\ n \quad where\ k = (-b) \qquad here\ k = -5$
   $[5 + (-5)] mod\ 8 = 0$
2. $b \times k = 1\ mod\ n \quad where\ k = b^{-1} \qquad here\ k = 5$
   $[5 \times 5] mod\ 8 = [25] mod\ 8 = 1$

5a. a. Apply the procedure to calculate the GCD using Euclidean algorithm and determine the GCD of (1160718174, 316258250).

```
Dividend        Divisor         Quotient Remainder
a = 1160718174  b = 316258250   q1 = 3   r1 = 211943424
b = 316258250   r1 = 211943424  q2 = 1   r2 = 104314826
r1 = 211943424  r2 = 104314826  q3 = 2   r3 = 3313772
r2 = 104314826  r3 = 3313772    q4 = 31  r4 = 1587894
r3 = 3313772    r4 = 1587894    q5 = 2   r5 = 137984
r4 = 1587894    r5 = 137984     q6 = 11  r6 = 70070
r5 = 137984     r6 = 70070      q7 = 1   r7 = 67914
r6 = 70070      r7 = 67914      q8 = 1   r8 = 2156
r7 = 67914      r8 = 2156       q9 = 31  r9 = 1078
r8 = 2156       r9 = 1078       q10 = 2  r10 = 0
```

GCD=1078

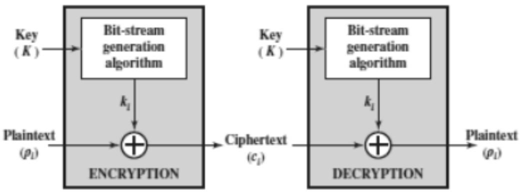
5M

5b. Distinguish between block cipher and stream cipher with examples

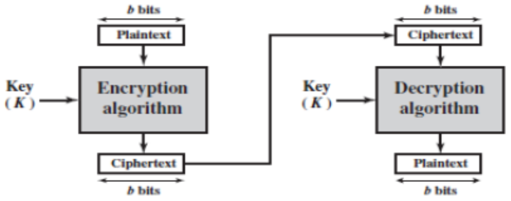
Difference between stream cipher and block cipher:

Stream cipher	Block cipher
1. Processing or encoding of plain text is done bit by bit.	1. Processing or encoding of the plaintext is done as a fixed length block one by one. E.g. 64 or 128 bit in size
2. Bits are processed one by one in a chain	2. A pad is added to short length block
3. Different key bit is used to encrypt each of the bits.	3. Same key is used to encrypt each of the blocks.
4. E.g. One Time Pad, Vigenère cipher, Vernam cipher	4. E.g. DES (Data Encryption Standard) ,AES (Advance Encryption Standard)
5. It is usually very simple and much faster.	5. Usually more complex and slower in

5M

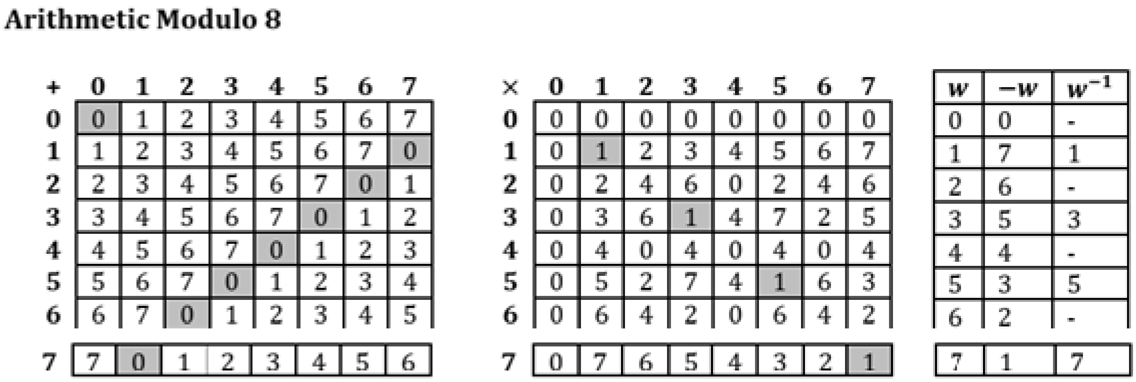
<table>
<tr>
<td></td>
<td>
<table>
<tr>
<td>6. Equally secure if properly designed
7. Statistically random
8. Requires less coding


Key
(K)
Bit-stream generation algorithm
k_i
Plaintext
(p_i)
ENCRYPTION
Ciphertext
(c_i)
Key
(K)
Bit-stream generation algorithm
k_i
DECRYPTION
Plaintext
(p_i)

</td>
<td>operation.
6. More secure in most cases.
7. Most block ciphers are based on fiestel cipher structure.
8. Requires more coding.


b bits
Plaintext
Key
(K)
Encryption algorithm
Ciphertext
b bits
b bits
Ciphertext
Key
(K)
Decryption algorithm
Plaintext
b bits

</td>
</tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>6a.</td>
<td>What are groups? Explain in detail with respect to its properties
➢ a set S of elements or “numbers”
• may be finite or infinite
➢ with some operation ‘.’ so G=(S,.)
➢ Obeys CAIN:
• Closure: a,b in S, then a.b in S
• Associative law: (a.b).c = a.(b.c)
• has Identity e: e.a = a.e = a
• has inverses a^{-1}: $a.a^{-1} = e$
➢ If also commutative a.b = b.a
• then forms an <b>abelian group</b></td>
<td>5M</td>
</tr>
<tr>
<td>6b.</td>
<td>Prove that if a×c ≡b×c (mod n) then a ≡ b (mod n) if c is relatively prime to n.
➢ <b>If a,b,c are all belongs to the set Z_n={0,1,2,…….n-1} and a is relatively prime to n.</b>
➢ <b>Then there exist a number a^{-1} such that a × a^{-1}≡ 1 (mod n)</b>
➢ <b>Now to (a × c) ≡ (b × c)(mod n) will apply multiplicative inverse to both sides.</b>
➢ <b>a^{-1}× (a × c) ≡ a^{-1}× (b × c)(mod n)</b>
➢ <b>∴ a ≡ b(mod n)</b>
➢ <b>Point to note that if a is not relatively prime to n then</b>
➢ <b>(a × c) ≡ (b × c)(mod n)</b>
➢ <b>e.g. (6 × 3) ≡ (6 × 7)(mod 8)</b>
➢ <b>Here (6 × 3) ≡ 2(mod 8) and (6 × 7) ≡ 2(mod 8) but 3 ≡ 7(mod 8)</b>
➢ <b>As 6 has no multiplicative inverse over modulo 8.</b></td>
<td>5M</td>
</tr>
<tr>
<td>7a.</td>
<td>Develop a set of additive and multiplicative tables for modulo-8.</td>
<td>5M</td>
</tr>
</table>



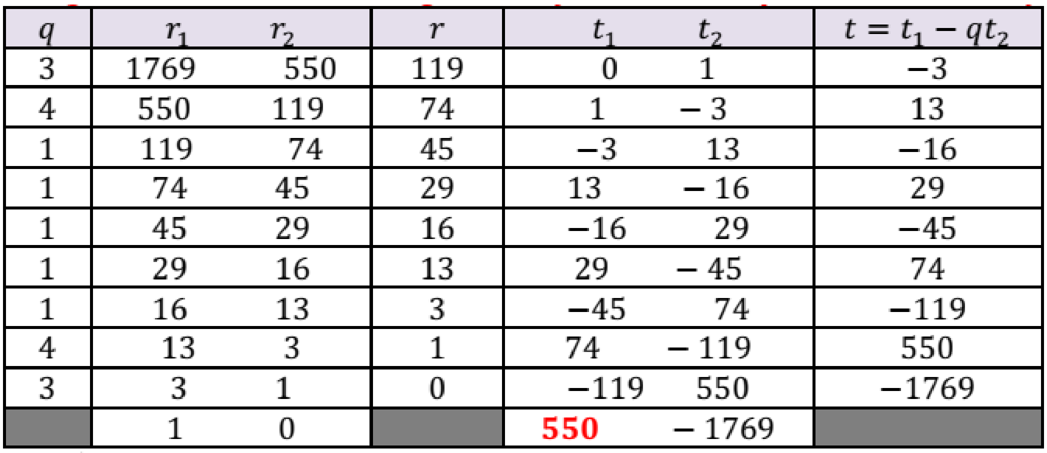
Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

w	$-w$	w^{-1}
0	0	-
1	7	1
2	6	-
3	5	3
4	4	-
5	3	5
6	2	-
7	1	7

7b. Using extended Euclidean algorithm, find the multiplicative inverse of 550 (mod 1769).



q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
3	1769	550	119	0	1	-3
4	550	119	74	1	-3	13
1	119	74	45	-3	13	-16
1	74	45	29	13	-16	29
1	45	29	16	-16	29	-45
1	29	16	13	29	-45	74
1	16	13	3	-45	74	-119
4	13	3	1	74	-119	550
3	3	1	0	-119	550	-1769
	1	0		**550**	-1769	

$550^{-1} mod\ 1769 = 550$

5M

CCI

HOD