Answer on Question #63939 - Math – Discrete Mathematics

Question

Suppose that you need to deliver the message "161803398" which is the pass key for a weapon activation to country X. Encrypt the message using Caesar cipher with the encryption key,
2
(2)mod9 n +
where
n =1, 2,...,9 , without being intercepted and decrypted by other countries.
(a) State the decrypted message.
(b) Determine the decryption key.
(c) Suggest an improvement to the encryption key to increase the encryption strength

Remarks:
Note the only variant of the correct (original) condition is possible
if the distorted text
2
(2)mod 9 n +
where
n =1, 2,...,9
is replaced by
(n+2·2) mod 10, where n =0, 1, 2,...,9
and
'(a) State the decrypted message'
is replaced by
'(a) State the encrypted message'.

Solution

(a) Each digit d of the encrypted message is calculated as $d = (n + 4)\ mod\ 10$, where n is the digit of the message to be encrypted, in the same position. Thus

$$1 \to (1 + 4)\ mod\ 10 = 5$$
$$6 \to (6 + 4)\ mod\ 10 = 0$$
$$1 \to (1 + 4)\ mod\ 10 = 5$$
$$8 \to (8 + 4)\ mod\ 10 = 2$$
$$0 \to (0 + 4)\ mod\ 10 = 4$$
$$3 \to (3 + 4)\ mod\ 10 = 7$$
$$3 \to (3 + 4)\ mod\ 10 = 7$$
$$9 \to (9 + 4)\ mod\ 10 = 3$$
$$8 \to (8 + 4)\ mod\ 10 = 2$$

and the encrypted message is "505247732".

(b) From the known digit d of the encrypted message, the corresponding digit n of the decrypted message can be found as $n = (n + 4 - 4 + 10)\ mod\ 10 = (d + 10 - 4)\ mod\ 10 =$
$= (d + 6)\ mod\ 10.$

(c) An example of the improvement to the encryption key is

$$d = (y \cdot n + x)\ mod\ 10,$$

where $n = 0,1,2,\dots,9$ is the digit of the message to be encrypted,

$d = 0,1,2,\ldots,9$ is the digit of the encrypted message,
the pair (x, y) is the encryption key, $y = 1,3,7,9$ (each y is such that y and 10 have no common divisors), $x = 0,1,2,\ldots,9$, if $y = 1$, $x \neq 0$ (assuming that each digit of the encrypted message has to be different from the corresponding digit of the decrypted message).
Thus, there exist 10·4-1=39 variants of the key.
Let $v = y^3 mod\ 10$, $u = v(10 - x)\ mod\ 10$. Then $(v \cdot x + u)\ mod\ 10\ = 0$,
$v \cdot y = y^4\ mod\ 10 = 1$ (v is reverse y modulo 10).
Consequently,
$(v \cdot d + u)\ mod\ 10 = (v \cdot y \cdot n + v \cdot x + u)\ mod\ 10 = n\ mod\ 10 = n.$

The other example of the improvement to the encryption key is

$$d_i = (n_i + x_i)\ mod\ 10,$$

where
$i = 1,2,3, \ldots 9$ is a position of the digit of the message,
$d_i = 0,1,2, \ldots 9$ is the digit of the encrypted message at the position i,
$n_i = 0,1,2, \ldots 9$ is the digit of the message to be encrypted, at the position i,
$x_i = 1,2, \ldots 9$ (assuming that each digit of the encrypted message has to be different from the corresponding digit of the decrypted message).
Thus, the encryption key is a sequence $\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9\}$.
This sequence can take $9^9 = 387420489$ values.
The decryption is $n_i = (d_i + 10 - x_i)\ mod\ 10$

Answer:

(a) The encrypted message is "505247732".
(b) The decryption key is $(d + 6)\ mod\ 10$, where $d = 0, 1, 2, \ldots, 9$
(c) The improvement to the encryption key:

Example 1

Encryption: $d = (y \cdot n + x)\ mod\ 10$, where $n = 0,1,2,\ldots,9$ for each digit. $y = 1,3,7,9$, $x = 0,1,2,\ldots,9$, if $y = 1$, $x \neq 0$. The pair (x, y) is the encryption key, there exist 39 variants of the key.

Decryption: $(v \cdot d + u)\ mod\ 10$, where $v = y^3 mod\ 10$, $u = v(10 - x)\ mod\ 10$.

Example 2

Encryption: $d_i = (n_i + x_i)\ mod\ 10$, where $i = 1,2,3, \ldots 9$ is a position of the digit of the message, $d_i = 0,1,2, \ldots 9$ is the digit of the encrypted message at the position i, $n_i = 0,1,2, \ldots 9$ is the digit of the message to be encrypted, at the position i, $x_i = 1,2, \ldots 9$. The encryption key is a sequence $\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9\}$, it takes $9^9 =$
$= 387420489$ variants.

Decryption: $n_i = (d_i + 10 - x_i)\ mod\ 10$.