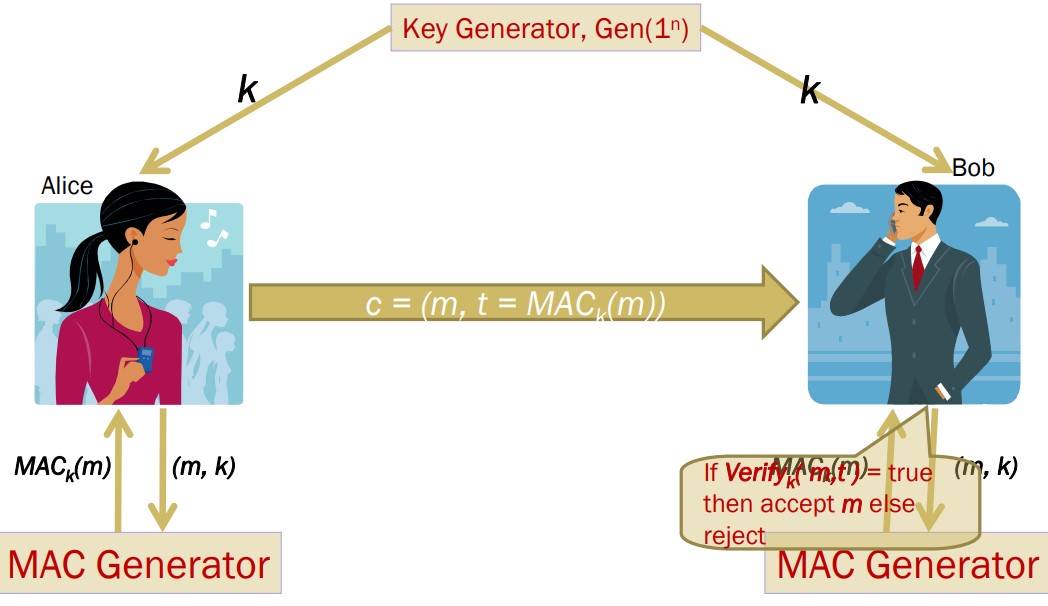
Message Authentication Code (MAC) **Theory:**



* A Key Generation Algorithm that returns a secret key k
* A MAC generating algorithm that returns a tag for a given message m. Tag t = MACk (m)
* A Verification algorithm that returns a bit
* b = Verifyk (m1, t1), given a message m1 and a tag t1
* If the message is not modified then with high probability, the value of b is true otherwise false

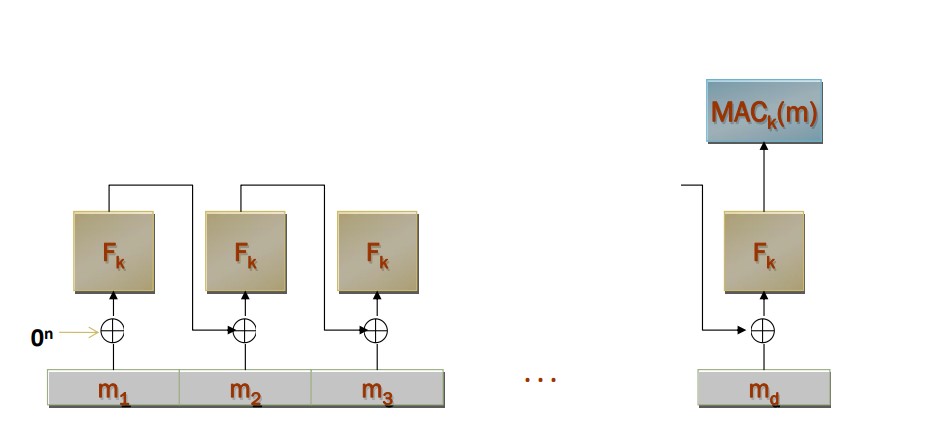
**Generating MAC:**

* Partition the message m to n sized blocks m1m2...mq
* Calculate MACk(m) = MACk(m1 ⊕ m2 ... ⊕ mq)

**Is this method secure?**

NO! We are authenticating the xor of the message blocks but not the message itself. So we can always choose a message whose xor value is the same as some other message.

**CBC-MAC:**



**Task:**

You are given 3 information: a message, key, and CBC-MAC signature. Your task is to verify whether the received message is valid or not.

|  |  |  |  |
| --- | --- | --- | --- |
| **Message** | **Key** | **MAC Signature** | **Validity** |
| I met an interesting turtle while  the song on the radio blasted away | b'\x01\xd8i\xa1^0\x9a<\x0 f\xf0\r\xc1\xdd\xd5\x89\xa 6' | ba4ecb8db45c6ae0 | Valid |
| I like to leave work after my eight-hour tea-break | b'\xa6+\x16\x9d-1\xda\x8 aV\xed\xf5\xf0cv\x04\x88' | f47e78c537fa1435 | Invalid |
| Her daily goal was to improve on yesterday | b'[\xc5\xbd\xe4z\xd1=E\x1 7-ku\x02=|=' | ddaf3152edbe868a | Valid |
| He found the chocolate covered roaches quite tasty | b'5"k\xff\x81a\x9b 7\x8c>\xb7\xb9\xdcu\xaa' | 9d30d856f84489a8 | Invalid key size |
| After fighting off the alligator, Brian still had to face the anaconda | b'\xa1\xfcw"?3\x91\x1c\t\x 9c\x91\xe2He\x935' | b9d173e05bbf7738 | Valid |
| He decided to count all the sand on the beach as a hobby | b'\xa7\x83@\xde\xbf\xb49 4\xee\x84\x1e-\xc8A\xf9:' | 6355e471bd9930a1 | Valid |
| The sign said there was road work ahead so he decided to speed up | b'2\xcbv\xdcU6\x99\xb6.\x a7\xea\xeb\xaf\x10\xc7\x9 0' | 9fbafc75e0a5056a | Valid |
| Send 500$ to this account 6589415651548 | b'\xc3\xea\x99e\xaal\xab\ xd4\x9b\xf9\xb4Z\x19\xed \xcf\xcb' | 35273149636aca35 | Valid |
| Garlic ice-cream was her favorite | b'\x05\xf9\x83\x9d\xb7\xb  6\xc3\xb8\x9e\xc5\xd9\xd  8\x07]\xc6\xb3' | dc2de1e07b71d391 | Invalid |
| I'd rather be a bird than a fish | b'\x84YY\xf0\x02GU\xa4L D\xd5\x85!A\xc2c' | 5e191d02aa5fc0b1 | Invalid |

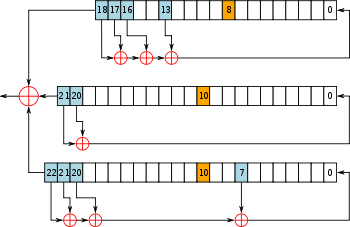
A5/1

**Theory:**

A5/1 consists of 3 shift registers.

X: 19 bits

Y: 22 bits Z: 23 bits



**Procedure:**

**Encrypt the following plaintext:**

|  |  |  |
| --- | --- | --- |
| **Plaintext** | **64-Bit Key** | **Ciphertext** |
| It is alive | 0011000001111111011110001  011011010011010000001000  011101101101011 | 001100011111010101101111111100101  00000010000000001111110110000110  000101110011111101101101000011101  0001 |
| Snap out of it | 111001101010101001110110  101000000100110011101101  1000001011001010 | 00110011101000100111100100000001  101000111111001101111110001101101  01100000001000111101000001101011  111111000000011101111101100011110  100 |
| I am as mad as hell and I am  not going to take this anymore | 001110101100110001000111  110111000111001100101101  1010100111001011 | 1110010100111000101010111001100  1101101111111001101011100000001  0011010000010101010001101110101  1010010111110110100000111000111  1010101110101010111000001111000  1001001111110110110010011010011  0000010001010001110000000010101  0011011010010110000010101011000  1110101011001000000000010101001  0001001111001110010101000101010  0010100101001100101011011010111  0010110011101100111000101011000  0110111011011010001001011111000  1110110110001001010011111010110  1111001101100111001010011000101  0111011111111100001000001101101  1111010111111101000101011111010  0111110001100010001000111110100  100110000011 |
| Bond James Bond | 110100000011110011001111  000000110011100100110000  0010110011100111 | 11101111000000100101011101001110  110011111101111101000111110100100  11011100011000011001011010110110  10111000000101000101111010111001  10110 |
| Love means never having to say you're sorry | 011111000010101100001010  111110011100000111000000  0001001101110110 | 1011011000100111010100101111010  1011111111010001000000010001110  0010110011110110101001001010000  0100011100000011100000111010110  0110010110101011010111101110111  0000100111110001111110001011101  1001000000100010000100001001101  0000011000101010000111011101101  0010110100111011011101000010001  0101011000011110100111100001000  1001010010000011110101110000001  0110001111111100110010100111110  1110110000000111010001011001 |

**Decrypt the following Ciphertext:**

|  |  |  |
| --- | --- | --- |
| **Ciphertext** | **64-Bit Key** | **Plaintext** |
| 101100001100101111010100  100100100010111010100001 | 100000000111100100000011  101011000011110010010100  1011001111000111 | **Nobody** |
| 01100001010000010000001  011101011000101000110011  00111111100100011 | 1100010111111111101000001  000110011010100100100111  011001000001100 | **KillBill** |
| 101001110100100101101011  01110111 | 001011001001100111100101  1100010100111010111011111  000010100010010 | **Bond** |
| 100011110111100000010000  111001000000110011111000  101011111001010000100110  101011101001010001011001  111110101100100 | 0001101101111111100111011  101010100000100111111100  011010010111010 | **Optimus@@ äÒÚ** |
| 1010111111111001100101000  100000111110010011000000  011010011010000111001010  0010010 | 111000000001100010111011  000010101110110101110000  1110110110000100 | **Darthvader** |