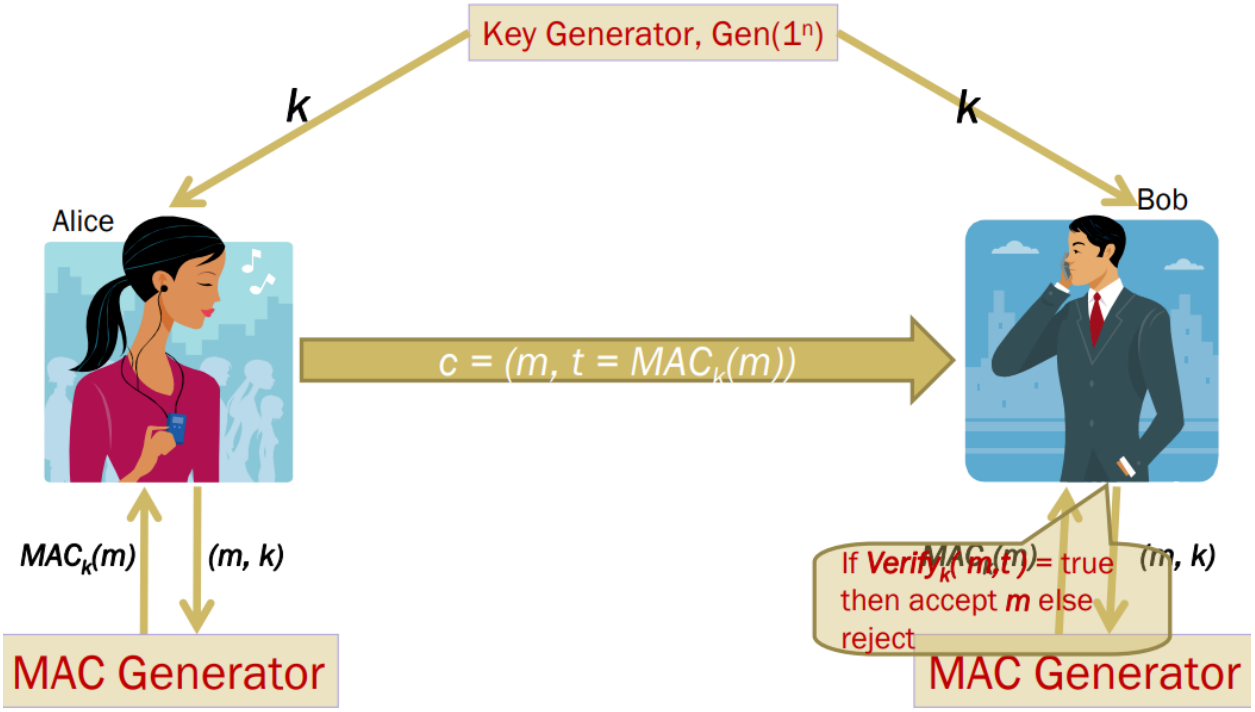
Message Authentication Code (MAC)

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

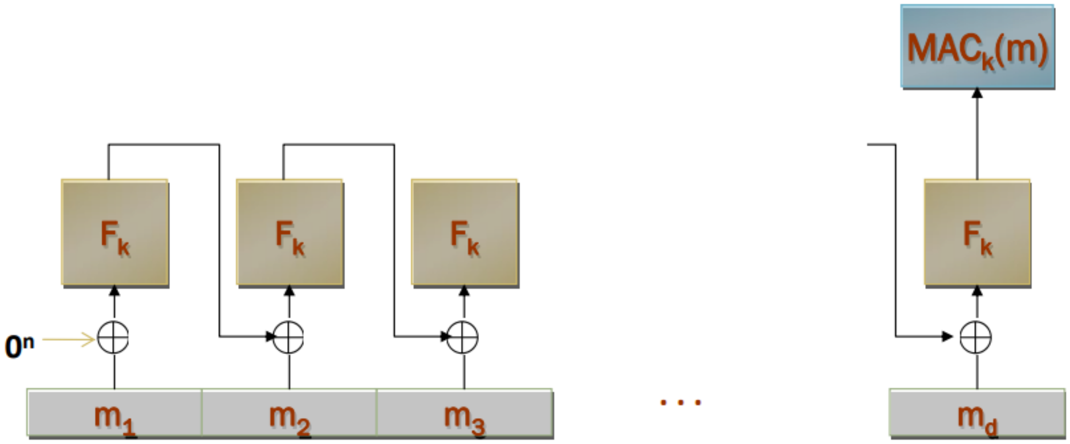
Generating MAC:

- 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<\x0f\xf0\r\xc1\xdd\xd5\x89\xa6'	ba4ecb8db45c6ae0	Yes
I like to leave work after my eight-hour tea-break	b'\xa6+\x16\x9d-1\xda\x8aV\xed\xf5\xf0cv\x04\x88'	f47e78c537fa1435	No
Her daily goal was to improve on yesterday	b'[\xc5\xbd\xe4z\xd1=E\x17-ku\x02=|='	ddaf3152edbe868a	Yes
He found the chocolate covered roaches quite tasty	b'5"k\xff\x81a\x9b7\x8c>\xb7\xb9\xdcu\xaa'	9d30d856f84489a8	Yes
After fighting off the alligator, Brian still had to face the anaconda	b'\xa1\xfcw"?3\x91\x1c\t\x9c\x91\xe2He\x935'	b9d173e05bbf7738	Yes
He decided to count all the sand on the beach as a hobby	b'\xa7\x83@\xde\xbf\xb494\xee\x84\x1e-\xc8A\xf9:'	6355e471bd9930a1	Yes
The sign said there was road work ahead so he decided to speed up	b'2\xcbv\xdcU6\x99\xb6.\xa7\xea\xeb\xaf\x10\xc7\x90'	9fbafc75e0a5056a	Yes

Send 500$ to this account - 6589415651548	b'\xc3\xea\x99e\xaal\xab\xd4\x9b\xf9\xb4Z\x19\xed\xcf\xcb'	35273149636aca35	Yes
Garlic ice-cream was her favorite	b'\x05\xf9\x83\x9d\xb7\xb6\xc3\xb8\x9e\xc5\xd9\xd8\x07]\xc6\xb3'	dc2de1e07b71d391	No
I'd rather be a bird than a fish	b'\x84YY\xf0\x02GU\xa4LD\xd5\x85!A\xc2c'	5e191d02aa5fc0b1	No

Procedure:

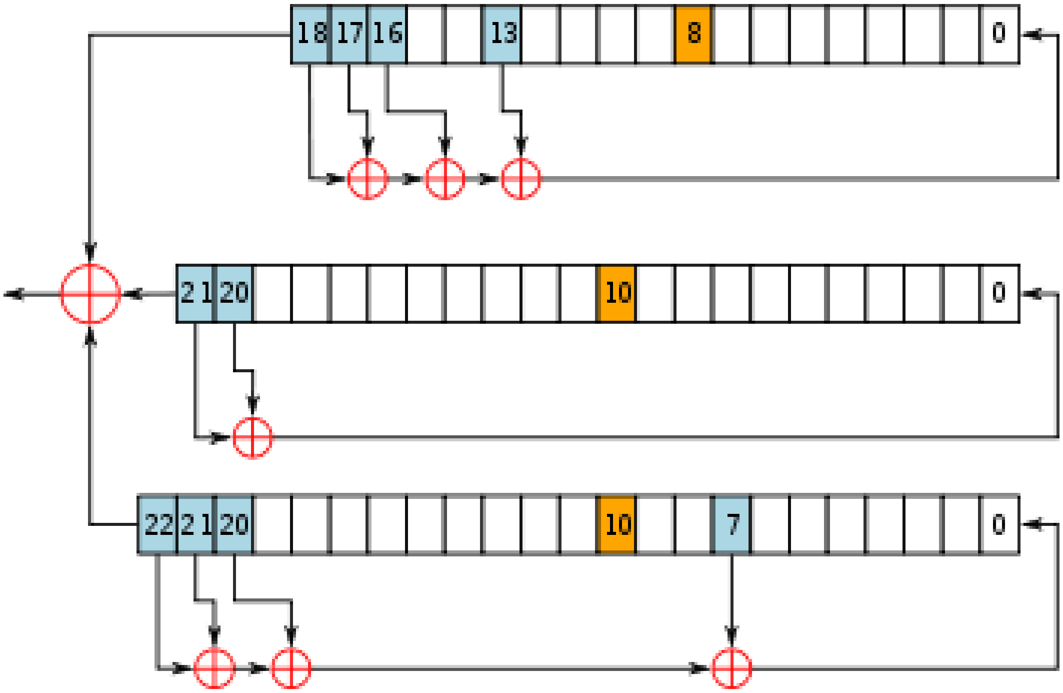
Colab Notebook Link for this lab:
https://colab.research.google.com/drive/1y0Za5ASOThcuahg7mxysdnd7QOEszlxj?

1. Create a cmac object as shown using **key**
2. Update() the created object with your received message
3. Generate the MAC signature using finalize() function
4. Finally, print the decoded version of the signature and match it with your given signature.

A5/1

Theory:

A5/1 consists of 3 shift registers.
X: 19 bits
Y: 22 bits
Z: 23 bits



Procedure:

Colab Notebook Link for this lab:
https://colab.research.google.com/drive/1y0Za5ASOThcuahg7mxysdnd7QOEszlxj?

1. **Complete** the encrypt() and decrypt() functions
2. Test your work by encrypting any plaintext and decrypting the found ciphertext

Encrypt the following plaintext:

Plaintext	64-Bit Key	Ciphertext

It is alive	0011000001111111011110001
	0110110100110100000001000
	01110110110101 1
		00110001111101010110111
		11111001010000001000000
		00011111101100001100001
		01110011111101101101000
		0111010001

Snap out of it	1110011010101010011101101010000001001100111011011000001011001010	00110011101000100111100100000001101000111111001101111110001101101011000000010001111010000011010111111110000000111011111011000111 10100
I am as mad as hell and I am not going to take this anymore	0011101011001100010001111101110001110011001011011010100111001011	1110010100111000101010111001100110110111111100110101110000000100110100000101010100011011101011010010111110110100000111000111101010111010101011100000111100010010011111110110110010011010011000001000101000111000000001010100110110100101100000101010110001110101011001000000000010101001000100111100111001010100010101000101001010011001010110110101110010110011101100111000101011000011011101101101000100101111100011101101100010010100111110101101111001101100111001010011000101011101111111110000100000110110111110101111111010001010111110100111110001100010001000111110100100110000011
Bond James Bond	1101000000111100110011110000001100111001001100000010110011100111	111011110000001001010111010011101100111111011111010001111101001001101110001100001100101101011011010111000000101000101111010111001101 10
Love means never having to say you're sorry	0111110000101011000010101111100111000001110000000001001101110110	10110110001001110101001011110101011111111010001000000010001110001011001111011010100100101000001000111000000111000001110101100110010110101011010111101110111000010011111000111111000101110110010000001000100001000010011010000011000101010000111011101101001011010011101101110100001000101010110000111101001

		11100001000100101001000001111010111000000101100011111111001100101001111101110110000000111010001011001

Decrypt the following Ciphertext:

Ciphertext	64-Bit Key	Plaintext
101100001100101111010100100100100010111010100001	1000000001111001000000111010110000111100100101001011001111000111	Nobody
0110000101000000100000010111010110001010001100110011111110010001 1	110001011111111101000001000110011010100100100111011001000001100	KillBill
10100111010010010110101101110111	001011001001100111100101110001010011101011101111000010100010010	Bond
100011110111100000010000111001000000110011111000101011111001010000100110101011101001010001011001111110101100100	000110110111111100111011101010100000100111111100011010010111010	Optimus@@ äÒÚ
1010111111110011001010001000001111100100110000000110100110100001110010100010010	1110000000011000101110110000101011101101011100001110110110000100	Darthvader