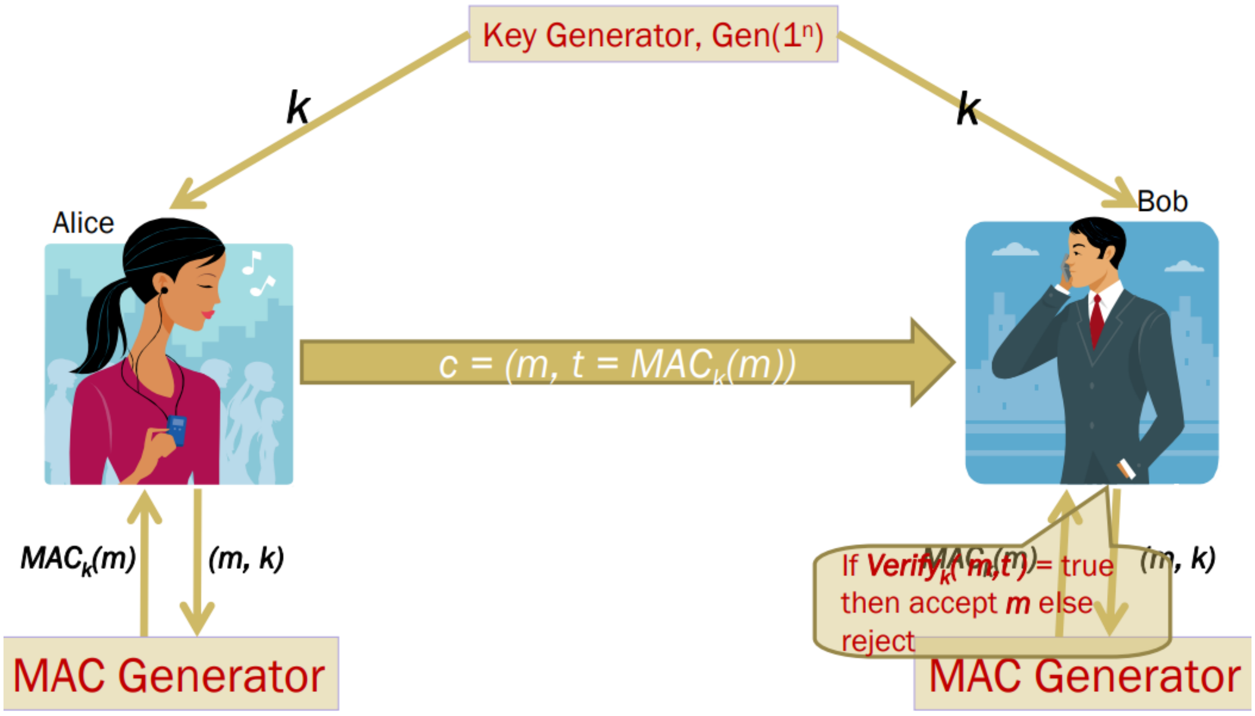
Message Authentication Code (MAC)

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 = Verify (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

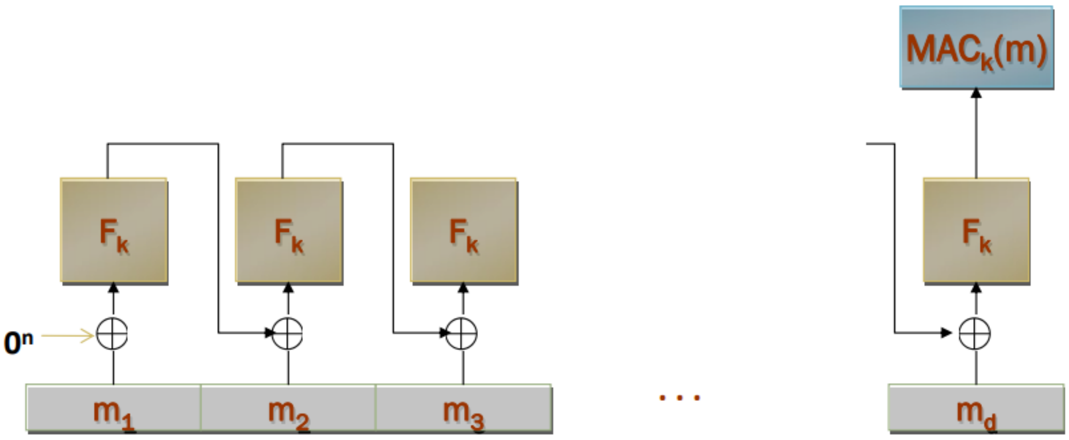
Generating MAC:

- 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 pieces of 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	valid
I like to leave work after my eight-hour tea-break	b'\xa6+\x16\x9d-1\xda\x8aV\xed\xf5\xf0cv\x04\x88'	f47e78c537fa1435	Invalid
Her daily goal was to improve on yesterday	b'[\xc5\xbd\xe4z\xd1=E\x17-ku\x02=|='	ddaf3152edbe868a	valid
He found the chocolate covered roaches quite tasty	b'5"k\xff\x81a\x9b7\x8c>\xb7\xb9\xdcu\xaa'	9d30d856f84489a8	valid
After fighting off the alligator, Brian still had to face the anaconda	b'\xa1\xfcw"?3\x91\x1c\t\x9c\x91\xe2He\x935'	b9d173e05bbf7738	valid
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	valid
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	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\xb6\xc3\xb8\x9e\xc5\xd9\xd8\x07]\xc6\xb3'	dc2de1e07b71d391	Invalid
I'd rather be a bird than a fish	b'\x84YY\xf0\x02GU\xa4LD\xd5\x85!A\xc2c'	5e191d02aa5fc0b1	Invalid

Procedure:

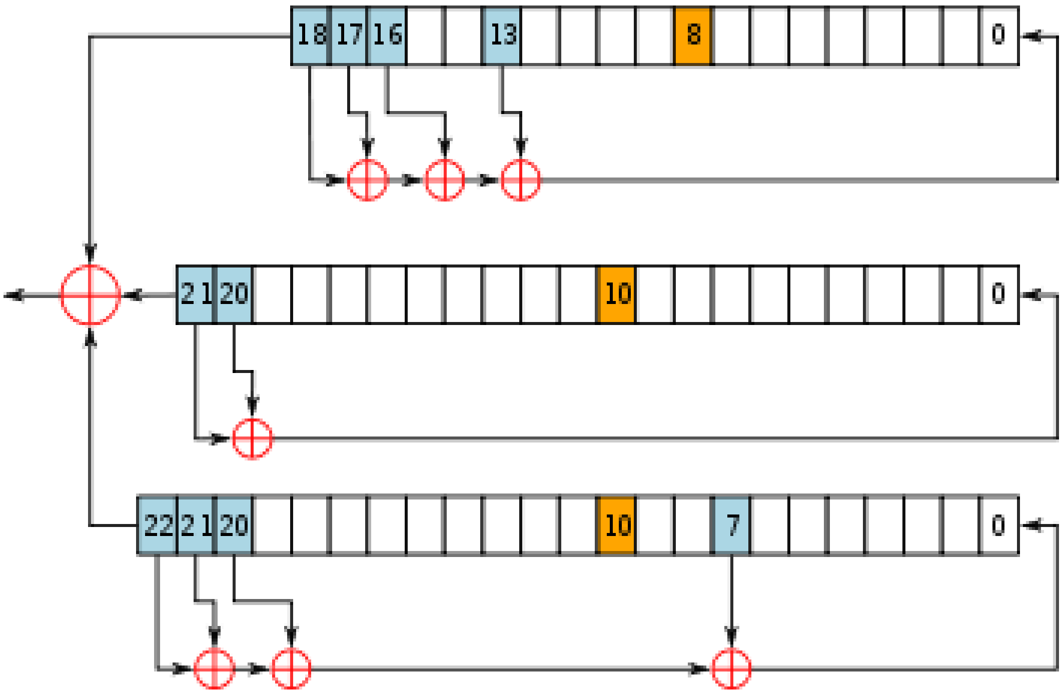
Colab Notebook Link for this lab: Lab 4 - CBC-MAC_A5_1 [Fall-2025]n

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:

Encrypt the following plaintext:

X=1110001100101001011

Y=0011000000010000001101

Z=10011101101111001001110

Prepare a function **A51(X, Y, Z, n)**

Plaintext	**Key stream** len(Plaintext) Use A51 algorithm (Binary)	**Ciphertext =** **Plaintext ⊕ key** (Binary)	**Plaintext =** **Ciphertext ⊕ Key** (String)
It is alive	11010100000011011111001111001100011100101001111100100011110011000001000111111010001001 01	10011101011110011101001110100101000000011011111010000101010000001111000100011000100000 0	It is alive
Snap out of it	1101010000001101111100111100110001110010100111110010001111001100000100011111110100010010101101010010100101010100111	1000011101100011100100101011110001010010111100000101011010111000001100011001010101000011010010100011101111010011	Snap out of it
I am as mad as hell and I am not going to take this anymore	110101000000110111110011110011000111001010011111001	100111010010110110010010101000010101001011111110010	I am as mad as hell and I am not going to take this anymore

	0001111001100000100011111101000100101011010100101001010100111001101001000100101101011101000000010111011110001110111001111010000000011010111011010010111100100100011000100111010111100100111011010110100110100111000111001001001101100100000001100101100000001000101000000110111110101101111011101000101001011110000110111000110110010010110000110001100111100100101100000100110000111011010110100011010001110111101110011110100101111	10000111011000111110010011011010000010100101000110011110101000001010011100001000011101100110001000010110100011011110110011010011001110111110111101100110001001110110100100011100111001111001111000010010000001100001111110101000000111110100110100101011001100011010001111001100110101001110110100101001010101010100000001010010010010001011000000101101010101111001010010100111100110000001010011111111100011100110000100111101001010	
Bond James Bond	11010100000011011111001111001100011100101001111100100011110011000001000111111010001001010110101001010010101001110011010 0	10010110011000101001110110101000010100101101010101000010101000010111010010001001000001010010100000111101110010010101000 0	Bond James Bond
Love means never having to say you're sorry	110101000000110111110011110011000111001010011111001000111100110000010001111110100010010101101010010100101010011100110100100010010110101110100000001011101111000111011100111101000000001101011101101001011110010010001100010011101011110010011101101011010011010011100011100100100110110010000000110010110000000100010100000011011111010110111101110100001	100110000110001010000101101010010101001011110010010001101010110101111111110001001000001010000010000110111110100010101000111111011010010111100100001001111100001111011010110011010011001000111110111010001100010111010110000111101110111011110010010001101010011011000110011100111010010111111001010101110001000010110011101100010100001111100111110101000	Love means never having to say you're sorry