CBC-MAC FUNCTIONS:

1. **CBC_MAC-**

   `Function to create Message Authentication code of given message`

Parameters	Datatype	Description
msg	str	Plaintext
key	str	Randomly chosen key
g	int	Generator
p	int	Prime
BLK_SIZE	int	Size of each msg block

Return:
`(str) : MAC tag of plaintext`

Called by:

- `CCA_ENC`
- `verifyMAC`

Caller of:

- `decimalToBinary`
- `binaryToDecimal`
- `PRF`

2. **verifyMAC-**

   `Function to authenticate MAC by creating new tag of msg and comparing with old tag received`

Parameters	Datatype	Description
msg	str	input whose tag is to be authenticated
key	str	Key used to create tag
tag	str	Tag against which new tag will be matched
g	int	Generator

p	int	Prime
BLK_SIZE	int	Size of each msg block

Return:
(bool): True if tag matches, False if tag doesn’t match

Called by:

- CCAAuthDec

Caller of:

- CBC_MAC