CCA-SECURE ENCRYPTION FUNCTIONS:

1. CCA_ENC-

`Function to encrypt message then create tag of the cipher text`

Parameters	Datatype	Description
msg	str	Plaintext
key1	str	Key to use for encryption
key2	str	Key to use for tag creation
g	int	Generator
p	int	Prime
BLK_SIZE	int	Size of each msg block

Return:

```
(str): counter to use for decryption
(str): encrypted cipher
(str): tag of cipher to be verified
```

Called by:

`Main code`

Caller of:

- `ENC`
- `CBC_MAC`

2. CCAAuthDec-

`Function to authenticate and decrypt cipher text. If authentication fails, decryption is not done.`

Parameters	Datatype	Description
key1	str	Key to use for decryption
key2	str	Key to use for tag verification
cipher	str	Cipher to decrypt

tag	str	Tag against which new tag generated on cipher is to be matched
counter	str	Counter to use to encrypt cipher
g	int	Generator
p	int	Prime
BLK_SIZE	int	Size of each msg block

Return:
`(void)`

Called by:
`Main code`

Caller of:

- `verifyMAC`
- `DEC`