ENCRYPTION

BY: MOMIN CHAUDHRY

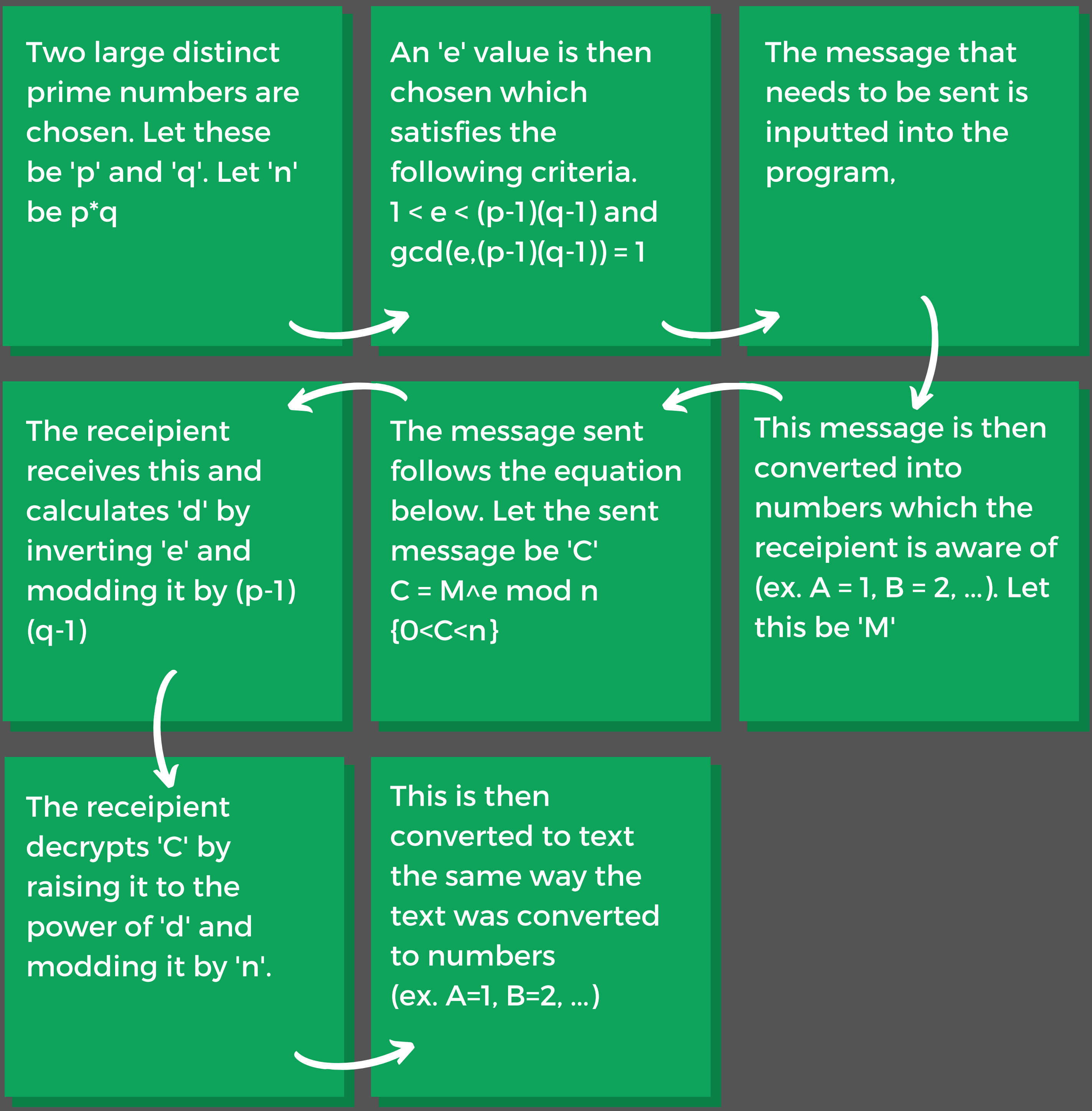
ABOUT ENCRYPTION

ENCRYPTION IS THE METHOD IN WHERE TEXT IS CONVERTED INTO A SECRET SCRAMBLED CODE WHICH CAN ONLY BE DECRYPTED BY THOSE WHO HAVE A KEY. ENCRYPTION HELPS TO SEND INFORMATION OVER PLATFORMS IN A SECURE WAY.

TYPES OF ENCRYPTION

- RSA
- TRIPLE DES
- AES
- FPE
- BLOW FISH
- TWO FISH

STEPS FOR RSA ENCRYPTION



Two large distinct prime numbers are chosen. Let these be 'p' and 'q'. Let 'n' be p*q

An 'e' value is then chosen which satisfies the following criteria.
$1 < e < (p-1)(q-1)$ and
$\gcd(e,(p-1)(q-1)) = 1$

The message that needs to be sent is inputted into the program,

This message is then converted into numbers which the receipient is aware of (ex. A = 1, B = 2, ...). Let this be 'M'

The message sent follows the equation below. Let the sent message be 'C'
$C = M^e \bmod n$
$\{0<C<n\}$

The receipient receives this and calculates 'd' by inverting 'e' and modding it by (p-1)(q-1)

The receipient decrypts 'C' by raising it to the power of 'd' and modding it by 'n'.

This is then converted to text the same way the text was converted to numbers
(ex. A=1, B=2, ...)