# **Elgamal based Digital Signature Algorithm**

## **Generation of Public key and Private key**

Timeline

Description automatically generated

This private key d = 16 is private to agent-X.

## **Generation of Digital Signature**

Timeline

Description automatically generated

The goal of Agent-Y is to check whether Y1 = Y2 or not.

Then only the source and integrity of the message is ensured.

For agent-X, the signature is Y1 and Y2

m 🡪 hash value

Timeline

Description automatically generated

Can the hacker creates Y1 and Y2 ??

To create Y1 and Y2 we need the private key d.

How to identify whether the hacker hacked the message / not ?  
 If the message is being altered, hash value will be changed V1 != V2.

## **Final Procedure**

Text, letter

Description automatically generated

Text, letter

Description automatically generated

Text

Description automatically generated