```
CIA
c 1 confidentiality
11 integrity
A I availability
Risk-likelihood and impact a threat will
       Will exploit vulnerability
    threat: numful event
              - mun-made
               -> natur
    vulnerability: weakness
    Ukelinood: 7. probability (exploit)
-Empac: $5$ (always measured in 4)
Commance = "Law" and "Requiations"
    GDOR = EN DUVALLY
    PU DSS = "credit cura"
Security Controls = "counter Measure"
    BIA, BCP, DRP
In cryptography, people spends their life to encrypt something that is NOT
meant to be broken "secret witing"
CMDrographic Algornims
                                                                            Original
thasin
- " Integrity"
                                                                             Fire
                                                                           Ayonthm
UNGN I FILE
                                                                            Marine
                                                                                 1 259.57.1
      Algorithm
                           1259 371
                                                           259 371
                 MDS .
       marrine
                                                                     MATCH
Hush does not care if you can see or read it, it only
 ares if you are going to mess with it!
                                                                ALGORIHM # MDS /SHA
Algorium to remember for mash:
                                       * NOT REVERSIBLE
                                                         1). Symmetic: RCS, AES, 3DES, DES
                                       * Fixed Size
1) MDS
                                                         2). Asymmetic: RSA, DH, ECC
J SHA
                                     Algorium
   + SHA 28
   " SHA 256
                                      machine
                                               How does receptions
   + SHA SIZ
                                               yet lopy of the single
Symmetric icey = "single"
  requires a lley
  11. 215
  2). AES
 2). DES/3DES
                  + method starts with
 private key
- incurption
                    receiver! Not sender
                                                               Algoritm
+ confidentiality
```

```
CIA
c 1 confidentiality
11 integrity
A I availability
Risk-likelihood and impact a threat will
        Will extloit vulnerability
     threat: numful event
               - mun-made
                -> natur
    vulnerability: weakness
    Ukelinood: 7. probability (explose)
-Impact: $5$ (always measured in 4)
Comprance = "Law" and " regulations"
    GDOR = EU DIVALY
    PU bss = "crèdit cura"
Security Controls = "counter Measure"
    BIA, BCP, DRP
In cryptography, people spends their life to encrypt something that is NOT
meant to be broken "sever witing"
Cyprographic Algornims
                                                                            onginal
t hasn
- " Integrity"
                                                                             File
                                                                          Ayonthm
                                                                            Marine
ungmal File
                                                                                 1259.57
      Algorithm
                           1259 371
                                                          259.3?!
                 MDS .
       maurine
                                                                    MATCH
Hun does not care if you can see or read it, it only
cares if you are going to mess with it!
                                                                ALGORIHM # MDS /SHA
Algorism to remember for nash:
                                       * NOT REVERSIBLE
                                                         1). Symmetic: RCS, AES, 3 DES DES
                                       * Fixed Size
1), MDS
                                                        2). ASYMMETIC: RSA, QH, ECC
J. SHA
                                     Algorium
   4 SHA 28
   - SHA 256
                                      Machine
                                               How does recedient
   + SHA SIZ
                                               yer lopy of the single
Symmetric key = "ingle"
  requires a 1 Ley
  11. 215
  2). AES
  2). DES/3DES
                  + muhod sturs with
 private key
inuyphon
                    receiver! Not sender

    Confidentiality
```

```
CIA
    confidentiality
     integrity
A I availability
Risk-likelihood and impact a threat will
        Will extroit vulnerability
    threat: numful event
               → man-made
               -> natur
    vulnerability: weakness
    Ukelinood: 7. probability (exploit)
-Impact: $5$ (always measured in 1)
Commance = "Law" and " Requiarions"
    GDDR = EU Drivacy
    Pu oss = "crèdit cura"
Security Controls = "counter Measure"
    BIA, BCP, DRP
In cruptography, people spends their life to enumpt someoning that is NOT
meant to be broken "secret witing"
Cyprographic Algoriums
                                                                            Unginal
T-hasn
- "Integrity"
                                                                             File
                                                                           Ayonthm
UNGM I FILE
                                                                            Madine
                                                                                 1259.57
      Algorithm
                           1.259 .371
                                                           259.371
       marine
                 MOS .
                                                                     MATCHI
Hush does not care if you can see or read it, it only
cares if you are going to mess with it!
                                                                ALGORIHM # MDS /SHA
Algorium to remember for nash:
                                       * NOT REVERSIBLE
                                                         1). Symmetic: RCS, AES, 3 DES DES
                                       * Fixed Size
1) MDS
                                                         2). Asymmetic: PSA, Q 1+, Ecc
U SHA
                                     Algorium
   + SHA 28
                                     Machine
   × SHA 256
                                               How does receptions
   + SHA SIZ
                                               yet lopy of the single
                  "single"
Symmetric Key
 requires a lley
 11. 265
 2). AES
 2). DES/3DES
                  + method starts with
 private key
* unauption
                    receiver! Not sender
                                                               Algoritm
r confidentiality
```

```
c 1 confidentiality
    integrity
A I availability
Risk-likelihood and impact a threat will
       Will exploit vulnerability
    threat: numful event
               - man-made
               -> natur
    vulnerability: weakness
    Ukelinood: 7. probability (exploit)
- Impact: $5$ (always measured in 1)
Comprance = "Law" and "Requiations"
    GDDR = EU DIVALY
    PU DSS = "credit cura"
Security Controls = "counter Measure"
    BIA, BLP, DRP
In cryptography, people spends their life to encrypt someoning that is NOT
meant to be broken "secret witing"
Cyprographic Algoriums
                                                                             onginal
th hasn
- "Integrity"
                                                                             Au
                                                                           Ayonthm
                                                                             Madine
ungmal File
                                                                                  1259.57.1
                                                           259.3?
      Algorithm
                           1259 .371
       marine
                 MOS.
                                                                     MATCH!
Hush does not care if you can see or read it, it only
cares if you are going to mess with it!
                                                                ALGORIHM # MDS /SHA
Algorithm to remember for nush:
                                        * NOT REVERSIBLE
                                                          1). Symmetic: RCS AES, 3DES DES
                                        * Fixed Size
1) MDS
                                                         2). Asymmetic: RSA, Q1+, ECC
U SHA
                                     Algorium
   4 SHA 28
                                      Muchine
   SHA 256
                                               How does receptions
   + SHA SIZ
                                                yet opy of the single
                   "single"
symmetric icey - requires a ley
  11. 215
                             Ley
  2). AES
  2). DES/3DES
                  + mumod starts with
* private key
= incurption
                     ecciver! Not sender
* confidentiality
```