Ciencia de la computación

Seguridad – CCOMP8-1

Rodrigo Andre Cayro Cuadros

Para esta corta implementación de cifrado se usó un algoritmo parecido al de AES, con bloques de 16, donde cada bloque tiene una frase de cifrado diferente. Para la etapa de cifrado se multiplica por un número random, para descifrar se le aplica el proceso inverso que es la multiplicación de las llaves generadas (las llaves están puesta en un vector invertido):

Mensaje original:

```
cayrinsqui@DESKTOP-72E0CDQ /mnt/d/8vo semestre/Seguridad/practico g++ mycrypto.cpp ✓ 140 18:25:48
cayrinsqui@DESKTOP-72E0CDQ /mnt/d/8vo semestre/Seguridad/practico ./a.out ✓ 141 18:45:57
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever sin
ce the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five ce
nturies, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release o
f Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versio
ns of Lorem Ipsum.
```

Mensaje cifrado:

```
EL MENSAJE CIFRADO ES: 025840377403876034034037060108802482038080391003978037060108803570039100108803910038850403304144039960447701184037000
432904033040330447701184042920373704440042920089603108028560089603248029120282800896031360319202940030800324802940030800288400512015520176 0
016000051201856019360179201616018400161601856018560168001760016480140804620048400440005148050600510405016053240202401408033440488405016044 4
404796011520262804032041400421203924011520374403492041400115203528036360363603960011520429203848037370118403885040700370004329042550429204 2
180447701443042550118404255049880417104730043000417104902043000137604300050310468704687052030137604988043430600005800016000505005900050050 0
700016000575005250055000495005050016000580005200022220070401078011660105601056025300096800704026180228802220242000704021340242000416015210 1
430013910143001443015470143000416014560148201365014300150801313014820089603248031080310802996008960271600896028840271603024030240282803388 8
008960310804182013120475604961045920414101312039770451004100013120471504059046740397704469009800108001010010000032001050011600032001160011 1
000320010900097001070010100032001358004480162401694015680141400448016100156801414013860147001526014140154000448026460299702997028890124200 8
640197103132008640280802619031050086403105031590307804838043050483804141041000131204510045510475601312045510451004428049610131204182028350 3
186027270086402673027270297003132031590307802835027270310501188008640264602691026680073602231024840264502553007360266802392023230073602484 0
232302231025760118403885040700429204107011840373703996037370366304292042180410704070038850366300384013920145201344012120138001212013920139 2
012600132001236005280038401368012120207101843019950209001995020900195700680191902185021850191902090022040199501843019440194402178005760210 6
601980017820187201746019800185401818018000082800576013140348000960035700291003450009600336003330033600351003240029100342003150034500303003 3
000105603465036300105603828034320333301056016170188101782015840379501056039270325503596032240099203596032240313100992035340313103348031310 3
007035650313100992014430132600416009880131301508014820126101495013130150800416014950135201313013130278402760007680237602664026400278402328 0
252002640025200264002472007680182402664020520181801962005760131402016020700210601962005760201601746020700207001746018540363604140015840115 2
034920396003600011520392403996041040363601152041040363603564030030033000348003240036300096003570031500348003120009600300003030034500321003 4
000105603465036300105603828034320333301056016170188101782015840379501056039270325503596032240099203596032240313100992035340313103348031310 3
007035650313100992014430132600416009880131301508014820126101495013130150800416014950135201313013130278402760007680237602664026400278402328 0
252002640025200264002472007680182402664020520181801962005760131402016020700210601962005760201601746020700207001746018540363604140015840115 2
034920396003600011520392403996041040363601152041040363603564030030033000348003240036300096003570031500348003120009600300003030034500321003 4
000333003360009600336003510029400324003150034500312003150033000309000960034500333023460266802737022310262200232300736024840241502461023230 7
360149502484023000269101035002880072000873009270090900693008730096300909010260028800945009900089100972023400200002100022000206000640023600 2
020022800230002100022200220002300006400222001836005760136801998020520181801962005760131402016020700210601962008280002000020
```

Mensaje descifrado:

```
EL MENSAJE DECIFRADO ES: Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's sta
ndard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has
survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the
 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus P
ageMaker including versions of Lorem Ipsum.
```

Link del repositorio:

https://github.com/rodRigocaU/My-crypto