

Criptografía y Cifrados de Información Semestre I, 2025

Manuel Rodas 21509

Lab 1 – Encriptado y Decriptado de Texto

cipher1.txt, cifrado Caesar.

El mejor desplazamiento encontrado es: 23

Texto descifrado:
numestrolaberintodigitalenconstanteevolucionlaagilidadcriptograficacriptoagilidadparaabreviaresunmecanismodedefensacrucialosbrindalacapacidaddemodificarrapidamenteelusodealgoritmosyclavescriptograficosunaaccionnecesario
numestrolaberintodigitalenconstanteevolucionlaagilidadcriptograficacriptoagilidadparaabreviaresunmecanismodedefensacrucialosbrindalacapacidaddemodificarrapidamenteelusodealgoritmosyclavescriptograficosunaaccionnecesario
numeratriciormosalasfuturassamenazasdeciberseeuridad

El mejor desplazamiento encontrado es: 23

Texto descifrado:

nnuestrolaberintodigitalenconstanteevolucionlaagilidadcriptograficacriptoagilidadpara abreviaresunmecanismodedefensacrucialosbrindalacapacidaddemodificarrapidamen teelusodealgoritmosyclavescriptograficosunaaccionnecesariaparaanticiparnosalasfut urasamenazasdeciberseguridad

cipher2.txt, cifrado afín.

Los mejores valores encontrados son: a = 5, b = 15
Texto descifrado:
nejemplodelamecesidaddecriptoagilidadsepuedeextraerdelosataqueseartbleedugdelerrorrevelounadebilidadcrucialquepermitioalosatacantesleerlamenoriademilesdesistemasyrobarinformacionvaliosaasempresasquelograronrecuperarsera
pidamentefueronlasquedemostraroncriptoagilidadreemplazandorapidamentesusclavescriptograficasyalgoritmoscomprometidosporotrosnuevosysegurossteincidentesirvecomounclaruejemplodelaimportanciadelacriptoagilidadenmuestrabatallacontinacontralasamenzasdainanicadeciberseguridad

Los mejores valores encontrados son: a = 5, b = 15

Texto descifrado:

nejemplodelanecesidaddecriptoagilidadsepuedeextraerdelosataqueseartbleedugdeler rorrevelounadebilidadcrucialquepermitioalosatacantesleerlamemoriademilesdesiste masyrobarinformacionvaliosaasempresasquelograronrecuperarserapidamentefueronl asquedemostraroncriptoagilidadreemplazandorapidamentesusclavescriptograficasyal goritmoscomprometidosporotrosnuevosysegurossteincidentesirvecomounclaroejempl odelaimportanciadelacriptoagilidadennuestrabatallacontinuacontralasamenazasdina micasdeciberseguridad

cipher3.txt, cifrado Vigenére

La mejor Clave encontroida es: payaso Tocto descriferáto: aurqueel enrorhearbi leed se haso Jucío mados iemprehayunumevamena zenez lhori ionteboy la cuanti caes esa amena zaque puedent raves artodas nues tras defensa antes deque todo este perdido debenos adoptar la cripto agilidad para defendemos disportible en la apprincipa les solu cionados iemprehayunumevamena zenez lhori ionteboy la cuanti caes esa amenaz aiminente de la computación cuanti cayaes ta enque pere cia mente contecnic ascomos torno moder crybitater sindique y aestuanti que y aestuanti preparados computación cuanti caes esa acuanti caes esa acuan

La mejor clave encontrada es: payaso

Texto descifrado:

aunqueelerrorheartbleedsehasolucionadosiemprehayunanuevaamenazaenelhorizonte hoylacuanticaesesaamenazaquepuedeatravesartodasnuestrasdefensasantesdequeto doesteperdidodebemosadoptarlacriptoagilidadparadefendernosdisponibleenlasprinci palessolucionesdecriptografiaposcuanticapqcdelaactualidadlaevidenciadelaamenaza inminentedelacomputacioncuanticayaestaaquiespecialmentecontecnicascomostoren owdecryptlatersndlqueyaestanenjuegosndlesunmetodoenelqueserobandatoscifrados ysealmacenanhastaquelospiratasinformaticospuedandescifrarlosmastardeconunaco mputadoracuanticaestosignificaunaamenazainminentelosdatoscifradossegonlosestan daresactualesperoalmacenadosparaundescifradofuturoestaranenriesgoyaquelascom putadorascuanticaseventualmenteromperanlosmetodosdecifradoactualesporlotantos ndlesunabombadetiempoyunclarorecordatoriodelaurgenciadeactualizarnuestrosmeto dosdecifradoparaqueseansegurosparalacomputacioncuanticaelenfoquepqcabordalan ecesidaddecriptoagilidadconvulnerabilidadescomosndlquepresentanunpeligroclaroyp resenteahoraeselmomentodedarunsaltocuanticoennuestracriptografia