**Kivonat**

Innovatív kriptográfiai platform: Cryptorithm

A Cryptorithm egy online platform, amely úgy lett tervezve, hogy a felhasználók számára lehetővé tegye a hashelést, szövegek vagy képek transzformációját, titkosítását és dekódolását különböző algoritmusok segítségével, tárolja az eredményeket és lehetőséget ad ezek megosztására is más felhasználókkal. A platform zökkenőmentes élményt nyújt érzékeny adatainak védelméhez, miközben megadja a felhasználónak a szabadságot, hogy az igényeinek megfelelő módszert válassza.

A titkosítás létfontosságú szerepet játszik a bizalmas információk védelmében a mai digitális világban. A Cryptorithm segítségével a fejlett titkosítási technikák alkalmazásával biztosíthatja adatai adatvédelmét és biztonságát. Akár személyes üzeneteket, érzékeny dokumentumokat vagy értékes képeket kell védenie, a platform átfogó megoldást kínál.

A Cryptorithm egyik legfontosabb jellemzője a többféle titkosítási algoritmus támogatása. A különböző helyzetek különböző szintű biztonságot igényelnek, ezért az algoritmusok változatos választékát kínálom az egyedi igényeknek megfelelően. A széles körben használt AES-től (Advanced Encryption Standard) a robusztus RSA-ig (Rivest-Shamir-Adleman) és még sok másig, rugalmasan választhatja ki az igényeinek leginkább megfelelő titkosítási módszert.

A titkosítási funkciók mellett a Cryptorithm egy kiterjedt tudásbázist is kínál, ahol felfedezheti és megismerheti a különböző titkosítási algoritmusokat. Hiszem, hogy a titkosítás alapelveinek megértése elengedhetetlen ahhoz, hogy a felhasználó megalapozott döntéseket hozhasson adatai védelmével kapcsolatban. Az átfogó dokumentáció és informatív cikkek segítségével bővítheti ismereteit, és betekintést nyerhet a kriptográfia világába.

**Hasonló platformok, szoftverek összehasonlítása**

Cryptii: A Cryptii egy online titkosítási és dekódolási eszköz, amely algoritmusok széles skáláját támogatja. Különböző szimmetrikus és aszimmetrikus titkosítási algoritmusok közül választhat, többek között AES, RSA, DES és sok más algoritmusok közül. A weboldal emellett lehetőséget biztosít a kódolásra, a hashelésre és a tömörítésre is. A bevitel és kimenet között lehetőség van különböző rétegeket hozzáadni, így a két végpont között több algoritmus is alkalmazható.

Encode-Decode: Az Encode-Decode egy olyan weboldal, amely különböző algoritmusokhoz kínál titkosítási és dekódolási szolgáltatásokat. Támogatja az olyan népszerű algoritmusokat, mint a Caesar rejtjelezés, a Vigenère rejtjelezés, a ROT13 és még sok más. A weboldal egy egyszerű felületet biztosít, ahol beírhatja a szöveget, és kiválaszthatja a kívánt titkosítási vagy visszafejtési módszert.

A Cryptii és Encode-Decode platform sem ad leírást a használt algoritmusokról, így ezeket csak úgy lehet hatékonyan használni amennyiben ismerjük azokat, vagy más forrásokból tájékozódunk róluk.

CyberChef: A CyberChef egy hatékony online eszköz az adatmanipulációhoz és a titkosításhoz/dekódoláshoz. A műveletek széles skáláját kínálja, beleértve az olyan titkosítási algoritmusokat, mint az AES, RSA, XOR és még sok más. Támogatja továbbá a kódolást, a hashelést, a tömörítést és más adattranszformációkat.

Rumkin: A Rumkin egy olyan weboldal, amely kriptográfiai eszközök gyűjteményét kínálja, beleértve a titkosítási és dekódolási segédprogramokat. Különböző algoritmusokhoz kínál lehetőségeket, mint például a Caesar rejtjelezés, a Rail Fence rejtjelezés, a Playfair rejtjelezés és még sok más. Emellett kódolásra, hashelésre és steganográfiára szolgáló eszközöket is tartalmaz.

dCode: A dCode egy olyan online platform, amely titkosítási és dekódolási eszközök hatalmas gyűjteményét kínálja. Algoritmusok, titkosítások és kódolások széles skáláját fedi le, beleértve a klasszikus titkosításokat, modern titkosítási módszereket és speciális kódolásokat. Emellett kriptoanalízishez is kínál eszközöket.

Ezeken az oldalakon már több, részletesebb leírást lehet kapni az algoritmusokról, bár már kevésbé felhasználóbarátok, mint az első két platform.

**Bevezető**

Az internet korában, ahol az információk szabad áramlása és megosztása mindennapi tevékenységünk részévé vált, az adatbiztonság és a privát kommunikáció kiemelkedő jelentőséggel bír. Az egyre növekvő online fenyegetések és adathalászati támadások szükségessé teszik, hogy hatékony kriptográfiai algoritmusokat alkalmazzunk adataink védelme érdekében. A diplomadolgozatom célja egy olyan platform kidolgozása, amely lehetővé teszi a felhasználók számára, hogy különböző kriptográfiai algoritmusokkal titkosítsák avagy dekódolják a kívánt bemenetet, tárolják és megosszák az eredményeket. Ezek mellett némi betekintést is nyerhetnek a használt algoritmusok működésébe és történetükbe.

A 21. századi kriptográfia az információbiztonság terén jelentős áttörést hozott. Az egyre bonyolultabb és erőteljesebb számítógépek lehetővé teszik, hogy olyan titkosítási módszereket alkalmazzunk, amelyeket korábban elképzelhetetlennek tartottunk. Az aszimmetrikus titkosítás, a digitális aláírások és a kulcsszervezési protokollok olyan eszközöket kínálnak, amelyek segítségével az adatok biztonságosan átvihetők a kommunikációs csatornákon.

Az internetes biztonság szempontjából az adatok védelme nem csupán az egyénekre, hanem az egész társadalomra is kihat. Az egyre növekvő adatforgalom és az online szolgáltatások térnyerése a digitális korszak alapvető kihívásait jelenti. Az internetes bűnözők mindent megtesznek annak érdekében, hogy hozzáférjenek a személyes adatokhoz, pénzügyi információkhoz és üzleti titkokhoz. Ezért elengedhetetlen, hogy megfelelő intézkedéseket hozzunk az adatbiztonság érdekében, és a kriptográfia jelentős szerepet játszik ebben.

A diplomadolgozatom platformja olyan kriptográfiai algoritmusokat fog tartalmazni, amelyek ismertek, érdekesek, népszerűek vagy széles körben elterjedtek. A felhasználóknak lehetőségük lesz kiválasztani a számukra legmegfelelőbb módszert, attól függően, hogy milyen szintű biztonságra van szükségük és milyen jellegű adatokat szeretnének védeni.

A cél, hogy egy olyan platformot hozzak létre, amely segítségével az egyének hatékonyan védelmezhetik adataikat az interneten. A különböző kriptográfiai algoritmusok részletes leírását és azok alkalmazási területeit is elérhetővé teszi, hogy a felhasználók megfelelően tudják kiválasztani a titkosítási módszereket a saját igényeik és prioritásaik szerint.

A diplomadolgozatom további részeiben részletesen bemutatom a választott kriptográfiai algoritmusokat, azok működését és a biztonsági jellemzőiket. Emellett leírom a platform tervezését és implementációját, valamint a felhasználói felület funkcióit. Az eredményeket és a felhasználói visszajelzéseket is elemezni fogom annak érdekében, hogy megállapítsam a platform hatékonyságát és felhasználóbarát mivoltát.

Az internetes biztonság és az adatvédelem fontossága egyre nagyobb mértékben érint mindannyiunkat. A diplomadolgozatom platformja reményeim szerint hozzájárul a felhasználók biztonságérzetének növeléséhez és adataik védelmének erősítéséhez vagy legalább ennek törekvésére az online térben.

**Alkalmazás felépítése**

Backend: Python-szerveroldal, Flask-keretrendszer, SQLAlchemy-adatbázis

Frontend: HTML CSS JS Jinja2

**(Általam megvalósított szoftverek)**

Használjak könyvtárfüggvényeket inkább vagy implementáljam az algoritmusokat?

# Caesar, Affin, Hill, Morse, Bacon, URL enc/dec, Base32/64

# DES, RSA

# RC4, LFSR, A51, ROT13

# Rabin, SAEP

# Hash (MD5, SHA-1/256/384/512)

# Block Cipher (alg. AES-128/256, mode CBC/CTR, key rand/given, iv rand/given)

# Case transform (lower, upper, capitalize, inverse)

#? Kriptoanalízis, steganográfia

**Szoftver**

Python nyelv, VSC környezet

Use Case diagram, Osztálydiagram, Szekvencia diagram