Encryption Multi-tool

Stephen Smith

Multiple Encryption options

- Caesar cypher
- Substitution cypher
- DES encryption
- AES encryption

Each are symmetric and have configuration for the key used for encrypting and decrypting.

limitations

Caesar cypher and substitution cypher are limited to only alphabetic characters due to implementation and thus is limited to text files.

AES and DES can be applied to any file format, although the DES is not a cryptographically secure option due to the low entropy of its 8 byte key.

secret.txt

```
1   This is an example secret text to be encrypted by a cypher!
2   I don't think it changes punctiation though, does it?
3
```

secret.txt.enc

```
1   Guvf vf na rknzcyr frperg grkg gb or rapelcgrq ol n plcure!
2   V qba'g guvax vg punatrf chapgvngvba gubhtu, qbrf vg?
3
```

Usage

encryptor.py {'encrypt' | 'decrypt'} FILENAME {'a' | 'c' | 's' | 'd'}
"encrypt" or "decrypt" specifies the action on the selected file.
"a", "c", "s", "d" refer to the encryption options: AES, caesar, substitution, or DES respectively.

After selecting an encryption type, you will be prompted for a key based on the method chosen.
- Caesar cypher uses an int value from 1-25.
- Substitution cypher uses a string of alphabetical characters to substitute the alphabet, which must contain all alphabetical characters.
ex: ONABJFYVMCLEKRZPIGTDWHQXUS
It can also be left blank to generate a random key.
- DES uses an 8 byte key for encryption.
- AES uses a 32 byte key for encryption and a 16 byte initialization vector.