

# CS427 Final Project - Stream File Encryption & Key Management

Casey Colley

Robert Detjens

Lyell Read

CS 427, Winter 2022

## Contents

<b>Abstract</b>	<b>2</b>
<b>Definitions</b>	<b>3</b>
<b>Stream Encryption and Decryption (enc, dec)</b>	<b>4</b>
Primitives . . . . .	4
Formal Scheme Definition . . . . .	4
Security Proof and Reasoning . . . . .	4
<b>Key Generation and Storage (keygen)</b>	<b>8</b>
Primitives . . . . .	8
Password-Based Key Derivation Function 2 (PBKDF2) . . . . .	8
Formal Scheme Definition . . . . .	9
Security Proof and Reasoning . . . . .	9
Deriving keys from passwords . . . . .	9
Use of keyfile hashes . . . . .	10
<b>Conclusion and Discussion</b>	<b>10</b>
<b>Appendix A: Changelog</b>	<b>10</b>
<b>Appendix B: Feedback</b>	<b>10</b>

## Abstract

To demonstrate proficient Cryptographic knowledge gained from this course, our group designed a NOISE: Nice Ol' Interactive Stream Encryption. This is basically a key manager with built in encryption/decryption of messages with the keys within the manager. This project demonstrated: knowledge of the different definitions of security for different components (encryption schemes, pseudorandom permutations, and compression functions), ability to research further on what was taught in class (to find a suitable PRP, which ended up being AES), ability to write proofs for our cryptographic scheme, and ability to implement in code and test our cryptographic scheme. We wrote this program in Python and utilized a number of different libraries: PyAES, getpass, and docopt.

**NOTE:** Our Python scripts have a few small bugs that we were unable to iron out prior to submission, and will be broken if you try to run them. Please feel free to read through the code however! We started implementing our modified CTR but ran into complications. We have decided to use regular non-CCA secure CTR and add a MAC to ensure CCA security, but this has not been implemented yet.

## Definitions

## Stream Encryption and Decryption (enc, dec)

These define the Encryption and Decryption algorithms used by the program both to encrypt and decrypt the Master Key, and to encrypt and decrypt messages *with* the Master Key.

### Primitives

Our design utilizes a secure block cipher/PRP,  $F$ .  $F$  will be the [AES block cipher](#) with a 128-bit key. Our program utilizes a Python library for the AES block cipher implementation called [PyAES](#).

$\text{klen} = 128$ $\frac{F_{AES}(k, d) :}{\text{BLACK BOX}}$ $\frac{F_{AES}^{-1}(k, d) :}{\text{BLACK BOX}}$
--

### Formal Scheme Definition

Our symmetric encryption mode will be a modified CTR mode. For the Decryption algorithm, we don't really need to have  $r$  or  $c_0$  as it's simply concatenated with  $m_i$  but we have kept it in the definition to better show how our modification resembles true CTR mode. Additionally,  $r$  could be used to verify that the decryption was successful, as the resulting block would be  $m_i || r$ .

$\text{blen} = 128$	$\frac{\text{ENC}_{CTR}(k, m_1    \dots    m_l) :}{\begin{array}{l} r \leftarrow \{0, 1\}^{\text{blen}} \\ c_0 := r \\ \text{for } i = 1 \text{ to } l : \\ \quad c_i := F(k, m_i    r) \\ \quad r := r + 1 \% 2^{\text{blen}} \\ \text{return } c_0    \dots    c_l \end{array}}$	$\frac{\text{DEC}_{CTR}(k, c_0    \dots    c_l) :}{\begin{array}{l} r := c_0 \\ \text{for } i = 1 \text{ to } l : \\ \quad m_i := F^{-1}(k, c_i) [\text{blen}:] \\ \quad r := r + 1 \% 2^{\text{blen}} \\ \text{return } m_1    \dots    m_l \end{array}}$
---------------------	--	--

### Security Proof and Reasoning

We will prove that the encryption scheme of our key manager, a modified CTR mode, has security against chosen ciphertext attacks. We assume that  $F$  is a secure PRP.

To prove that a scheme has CCA security, we must prove that two random plaintexts (L & R) cannot be distinguished from each other, including any partial information, like so:

$\mathcal{L}_{\text{CCA-L}}^\Sigma$		$\mathcal{L}_{\text{CCA-R}}^\Sigma$
$k \leftarrow \Sigma.\text{KeyGen}$ $\mathcal{S} := \emptyset$		$k \leftarrow \Sigma.\text{KeyGen}$ $\mathcal{S} := \emptyset$
$\text{EAVESDROP}(m_L, m_R) :$ if $ m_L  \neq  m_R $ : return <b>err</b> $c := \Sigma.\text{Enc}(k, m_L)$ $\mathcal{S} := \mathcal{S} \cup c$ return $c$	$\approx$	$\text{EAVESDROP}(m_L, m_R) :$ if $ m_L  \neq  m_R $ : return <b>err</b> $c := \Sigma.\text{Enc}(k, m_R)$ $\mathcal{S} := \mathcal{S} \cup c$ return $c$
$\text{DECRYPT}(c) :$ if $c \in \mathcal{S}$ return <b>err</b> return $\Sigma.\text{Dec}(k, c)$		$\text{DECRYPT}(c) :$ if $c \in \mathcal{S}$ return <b>err</b> return $\Sigma.\text{Dec}(k, c)$

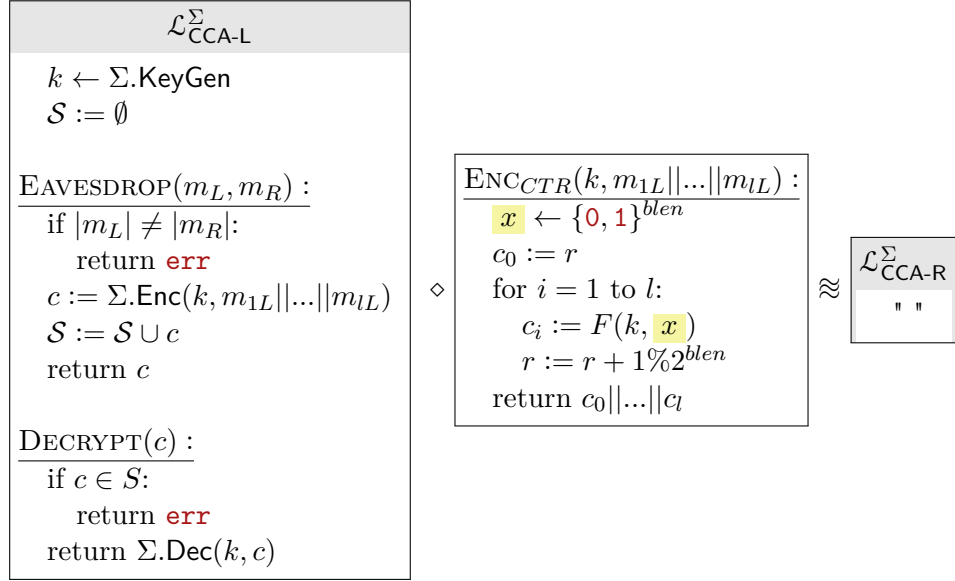
From here, we will walk through the proof for the left library.

$\mathcal{L}_{\text{CCA-L}}^\Sigma$				$\mathcal{L}_{\text{CCA-R}}^\Sigma$
$k \leftarrow \Sigma.\text{KeyGen}$ $\mathcal{S} := \emptyset$				
$\text{EAVESDROP}(m_L, m_R) :$ if $ m_L  \neq  m_R $ : return <b>err</b> $c := \Sigma.\text{Enc}(k, m_{1L}    \dots    m_{lL})$ $\mathcal{S} := \mathcal{S} \cup c$ return $c$	$\diamond$	$\text{ENC}_{CTR}(k, m_{1L}    \dots    m_{lL}) :$ $r \leftarrow \{0, 1\}^{blen}$ $c_0 := r$ for $i = 1$ to $l$ : $c_i := F(k, m_{iL}    r)$ $r := r + 1 \% 2^{blen}$ return $c_0    \dots    c_l$	$\approx$	" "
$\text{DECRYPT}(c) :$ if $c \in \mathcal{S}$ : return <b>err</b> return $\Sigma.\text{Dec}(k, c)$				

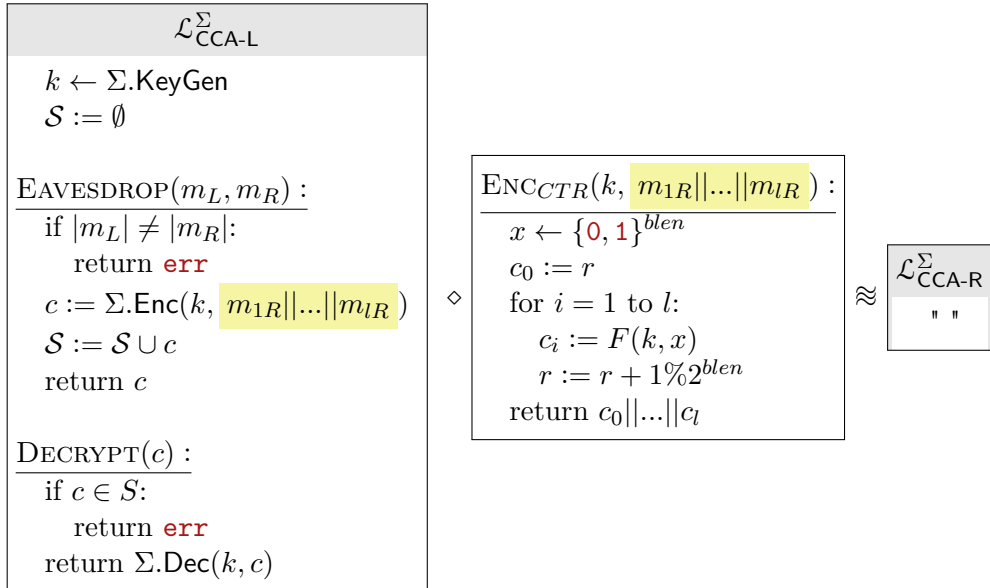
Next, we can turn our attention to the linked encryption scheme. Here we see that for each block, we calculate  $F(k, m_i || r)$  for the corresponding ciphertext block.  $r$  is sampled randomly, so the chance of collision is  $\frac{1}{2^{blen}}$ . However, we are doing counter mode, so  $r$  for each subsequent block in the message is deterministic, for  $l$  blocks in the message. Still, the rate of collision comes to  $\frac{l}{2^{blen}}$ . The  $l$  increases much slower than the  $2^{blen}$ , which means the rate of collisions is still negligible.

Because  $r$  is sampled randomly and has a negligible rate of collisions,  $m_i || r$  also has a collision rate of  $\frac{l}{2^{blen}}$  even when the same  $m_i$  is inputted. It does not matter what  $m_i$  is when we concatenate it

with  $r$  and put it through the PRP  $F$ . To illustrate this, we can apply the following transformation:



Now,  $m_{1L} || \dots || m_{lL}$  is not being used by the  $Enc_{CTR}$  function; we can change it to some other name without disrupting the function of the encryption scheme. We can rename this to  $m_{1R} || \dots || m_{lR}$  and inline it into the library.



Let's inline the whole linked function, and re-consider the right library.

$\mathcal{L}_{\text{CCA-L}}^\Sigma$		$\mathcal{L}_{\text{CCA-R}}^\Sigma$
$k \leftarrow \Sigma.\text{KeyGen}$ $\mathcal{S} := \emptyset$		$k \leftarrow \Sigma.\text{KeyGen}$ $\mathcal{S} := \emptyset$
$\text{EAVESDROP}(m_L, m_R) :$ <hr/> if $ m_L  \neq  m_R $ : return <b>err</b> $c := \Sigma.\text{Enc}(k, m_R)$ $\mathcal{S} := \mathcal{S} \cup c$ return $c$	$\approx$	$\text{EAVESDROP}(m_L, m_R) :$ <hr/> if $ m_L  \neq  m_R $ : return <b>err</b> $c := \Sigma.\text{Enc}(k, m_R)$ $\mathcal{S} := \mathcal{S} \cup c$ return $c$
$\text{DECRYPT}(c) :$ <hr/> if $c \in \mathcal{S}$ return <b>err</b> return $\Sigma.\text{Dec}(k, c)$		$\text{DECRYPT}(c) :$ <hr/> if $c \in \mathcal{S}$ return <b>err</b> return $\Sigma.\text{Dec}(k, c)$

Here we can see in this function, the left and right libraries are indistinguishable. For any calling program  $A$ , it will not be able to distinguish between the two libraries - aka, it will not be able to obtain any partial information from the scheme. Therefore, the scheme has CCA security, and by extension, has CPA security.

## Key Generation and Storage (keygen)

These define the functions that handle generation and storage of keyfiles used by the program. These keyfiles are generated with the function `KeyGen`, which samples a string of length `klen`. This sampling will come from the machine’s built-in random device, such as `/dev/urandom`.

These keyfiles are stored encrypted with a password that varies per keyfile. This “password encryption” is implemented by way of Password-Based Key Derivation Function 2 (PBKDF2). This will be expanded upon in the Primitives section.

The keyfiles are encrypted without a MAC as a MAC requires additional secret keys. Our goal is to encrypt with only one password-derived key, so encrypting and MAC’ing is not feasible. To compensate somewhat, a hash is appended to the keyfile before the whole keyfile is encrypted. More discussion on the security properties of this are discussed later.

## Primitives

The two biggest primitives we will define here is a hash function and PBKDF2.

We will also use the  $F_{AES}$  block cipher that we defined earlier. When we use  $F_{AES}$  in the **Stream Encryption and Decryption** section, the key it takes is the “master key” that is outputted from this section. When we use  $F_{AES}$  in here, it will not be used in the same way.

## Password-Based Key Derivation Function 2 (PBKDF2)

PBKDF2 is an established Key Derivation Function that will be doing the heavy lifting in turning a keyfile’s password into a usable “master key” to decrypt it. This function repeatedly calls a PRF to generate each block of the key. After this key is generated, we will use it to decrypt the keyfile.

PBKDF2 requires a pseudorandom function as part of its algorithm. In [RFC2898](#), an example PRF given is an HMAC. Instead, the PRF we will be using is our AES block cipher  $F_{AES}$  defined previously. A PRP is simply a PRF with additional requirements. Because of this, it’s still a PRF, so we shall be using it for our PBKDF2.

A few parameters are seen below.  $s$  is a salt that can be an arbitrary length (as it will be hashed down).  $klen$  is the desired length of the key. We can change this, however we are constricted to the key-lengths that our encryption algorithm can take, which is 128.  $blen$  is the fixed length of our PRF output. In this scheme, our PRF spits out 128-bit output. By using the same  $F_{AES}$  for both our PBKDF2 output and our encryption, we do constrict ourselves to specific input and output lengths throughout our program (namely, 128 bits).  $c$  is the number of iterations that the PRF should be applied per block. This should be a very large number.



```

klen := 128
blen := 128
c :=
PBKDF2(p, s):
  for i = 1 to (klen/blen):
     $U_1 := F_{AES}(p, s || i)$ 
     $T_i := U_1$ 
    for j = 2 to c:
       $U_j := F_{AES}(p, U_{i-1})$ 
       $T_i := T_i \oplus U_j$ 
     $T_i \leftarrow T_i$ 
  return  $T$ 

```

## Formal Scheme Definition

Our program relies on three secret keys: a key for encryption and decryption of a file, and two keys to generate a MAC for the encrypted file's contents.

The encrypted keys and their hash will be kept in a file, and the decrypted keys will be extracted and used internally within the program only. This is reflected below:

<p>KeyFile := KeyGen()</p>	<p><u>KeyGen():</u>  <math>p := \text{getpass}()</math>  <math>s \leftarrow \{0, 1\}^\lambda</math>  <math>K := \text{PBKDF2}(p, s)</math>  <math>key \leftarrow \{0, 1\}^\lambda</math>  <math>mac1 \leftarrow \{0, 1\}^\lambda</math>  <math>mac2 \leftarrow \{0, 1\}^\lambda</math>  <math>kh = \text{HASH}_{DM}(k    mac    mac2)</math>  <math>E := \text{ENC}_{CTR}(K, key    mac1    mac2    kh)</math>  return <math>E    s</math></p>	<p><u>DecryptKey():</u>  <math>p := \text{getpass}()</math>  <math>s := \text{Keyfile}[-\lambda :]</math>  <math>K := \text{PBKDF2}(p, s)</math>  <math>k, mac1, mac2, H := \text{DEC}_{CTR}(K,</math>  <math>keyH := \text{HASH}_{DM}(k    mac1    mac2)</math>  if <math>H \neq keyH</math>:  return <b>err</b>  return <math>k, mac1, mac2</math></p>
----------------------------	--	--

## Security Proof and Reasoning

### Deriving keys from passwords

We use the PBKDF2 algorithm to transform a keyfile's password into a 128-bit key used to decrypt the Keyfile. PBKDF2 uses our block cipher *FAES* for its PRF calls. We know that *FAES* is a secure PRP, and so, a secure PRF as well. We know this because to be a secure PRP, it has to be a secure PRF first, with additional requirements:

1. the inputs and outputs are distinct
2. the function is invertible

Additionally, the proving of both PRPs and PRFs are the [exact same library proof](#). Therefore, our *F<sub>FAES</sub>* is a secure PRF upon which we can build our PBKDF2.

TODO: rest of PBKDF2 defense <https://www.tarsnap.com/scrypt.html> <https://nvlpubs.nist.gov/nistpubs/Legacy/S108.pdf>

## Use of keyfile hashes

The actual keyfile itself contains three keys, as described above. These three keys are concatenated together and then hashed through our Davies-Meyer function. This hash is used as a verification that a) the password is correct, and b) the keyfile is not corrupted. If either of these conditions does not hold, then the program will return an error instead of the correctly-decrypted keys. While a MAC would be ideal here, a MAC requires the use of an additional key. We are unable to do that while continuing use a password to encrypt the keyfile.

The usage (or not) of a MAC for the key storage functions is not important. It is important for the encryption and decryption of files, as those are intended to leave the computer, where eavesdroppers could corrupt and edit the files before they get to their destination. However, for the storage of keyfiles on a single computer, the risk for corruption is a lot lower, and it's not imperative that the keyfiles have MACs computed for them.

## Conclusion and Discussion

In this report, we have methodically gone through each component of our key manager, including the encryption scheme, the Master Key generation and storage, and how we apply our encryption and decryption schemes to the KeyFile in a way that ensures that an attacker cannot gain partial knowledge of either the Master Key, the keys in the key manager, or the messages sent be NOISE.

## Appendix A: Changelog

Our draft was like this, we changed it to like this after receiving feedback.

## Appendix B: Feedback

“Good progress so far. I think it would be helpful to be clearer about what specific problem you’re trying to solve. It might help to differentiate your approach from other similar ones, and share design rationale. I admire your efforts to do a security proof but I see some bugs: 1. if “r” is  $\text{blen}$  bits long then there is no space left for m 2. decryption doesn’t check r, nor does it separate  $m||r$  3. This cannot be CCA secure  $\rightarrow$  I can drop the last ciphertext block and the result is still a valid encryption 4. It is a little bit more involved than you claim to derive the probability of collisions in r (since you care about collisions in r,  $r+1$ , ..  $r+L$ ). If you are really using passwords rather than true encryption keys, then you should give more details about how the password is converted to a key. Just saying Davies-Meyer doesn’t give me enough information (that’s like saying “I use CTR mode” without saying what the block cipher is), and it is probably not the ideal way to derive a key from a password anyway.”