Dokumentacja projektu archiwizer

Oprogramowanie kryptograficzne

Anna Reichel

14 listopada 2015

1 Opis projektu

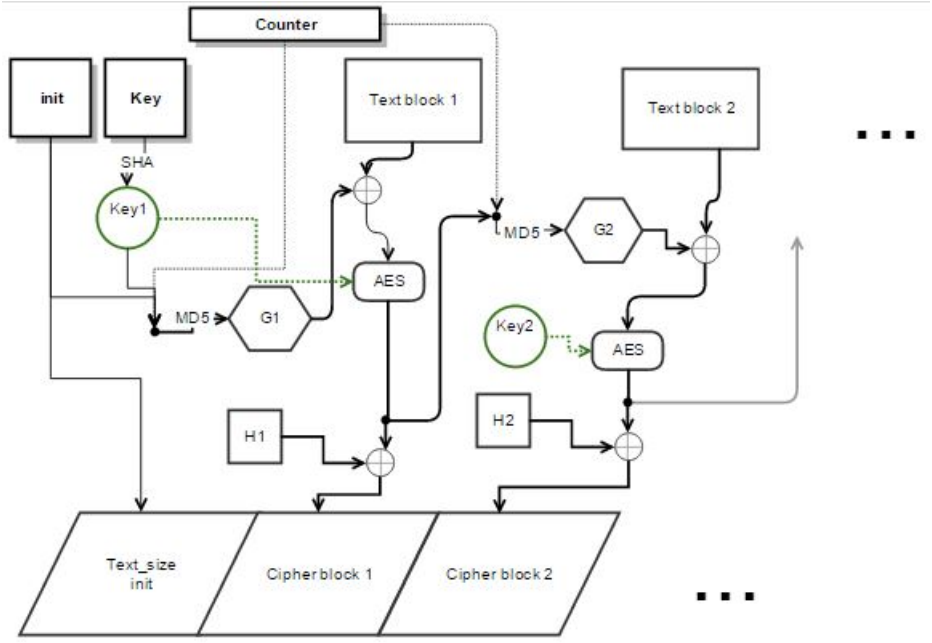
Celem projektu jest stworzenie aplikacji służącej do archiwizacji danych. Podczas pierwszego użycia aplikacji, obliczany na podstawie danych sprzętowych będzie identyfikator(ID) jednostki. Na podstawie ID, dystrybutor przydzielał będzie klucz produktu. Użytkownik będzie mógł stworzyć hasło do aplikacji. Aplikacja sprawdzać będzie, czy w już zarchiwizowanych plikach nastąpiły zmiany. W przypadku gdy pliki się zmieniły, archiwum będzie aktualizowane. Użytkownik wówczas zostanie poinformowany, w jakich plikach nastąpiły zmiany.

Dystrybutor aplikacji będzie wyposażony w dodatkowy program, który na podstawie ID generować będzie klucz produktu.

2 Szczegółowy opis

Przy każdym kolejnym uruchomieniu aplikacji weryfikowana będzie poprawność klucza produktu. W przypadku gdy klucz zgodny jest z ID, program zweryfikuje hasło dostępu użytkownika do archiwum. Następnie na podstawie pliku zawierającego strukturę katalogów, użytkownik będzie mógł wybrać plik i dokonać na nim zmian. Dodatkowo użytkownik będzie mógł zadać maksymalny rozmiar paczek zarchiwizowanych.

3 Schemat szyfrowania



Gdzie dokładniej:

- Key_1=SHA1(Key)

  Key_i=SHA1(Key_{i-1}), $i > 1$

- G_1=MD5(IV, Key_i, counter)

  G_i=MD5($Cipherblock_{i-1}$, Key_i, counter), $i > 1$

- H_i = SHA256(Key_i)

Użytkownik w czasie uruchomienia aplikacji podaje hasło główne (Key). W przypadku pierwszego uruchomienia aplikacji, wartość inicjująca IV jest losowana, w przeciwnym wypadku wartość odczytywana jest z wcześniej zapisanych plików. Następnie pliki dzielone są na paczki określonej długości, z których każda jest XORowana z wartością G_i i szyfrowana w trybie blokowym z użyciem algorytmu AES. Przed zapisem do pliku blok szyfrogramu XORowany jest z funkcją skrótu (SHA256) bieżącego klucza. Kolejne wartości G_i generowane są jako skrót MD5 na podstawie bieżącego klucza, tekstu szyfrogramu poprzedniej iteracji (w pierwszej iteracji wartości inicjującej IV) oraz G2.

4 Elementy opcjonalne

- Instalator
- Projekt w wersji okienkowej

5 Plan pracy

Plan pracy	
Zajęcia	**Etap – opis prac**
1	Implementacja metody generującej ID użytkownika, klucza produktu oraz weryfikującej poprawność klucza.
2	Implementacja podziału plików na paczki i szyfrowania plików
3	Implementacja metody szukającej zmian w plikach i zapisującej strukturę katalogu.
4	Oddanie projektu