Criptografía y seguridad
Práctica 2: Readme

Andrea Itzel González Vargas
Carlos Gerardo Acosta Hernández

Entrega: 20/03/17
Facultad de Ciencias UNAM

1. Modo de operación

El modo de operación utilizado en nuestra implementación de DES es el "Electronic Code Book" (ECB), dado que cada bloque de 64 bits es cifrado independientemente del resto. Lo elegimos por su simplicidad.

2. Uso del programa

Compilación

Para compilar el código fuente contenido en **des.c** es necesario utilizar las banderas -lm para el compilador *GCC*, pues hemos incluído la biblioteca *math* para llevar a cabo nuestra implementación. Un ejemplo:

```
$ gcc -lm des.c -o DES
```

Ejecución

Una vez obtenido el binario ejecutable, es necesario darle ciertos argumentos de entrada. En primer lugar, se especifica si hará un cifrado ('c') o un descifrado ('d'), luego una llave de longitud 8 y finalmente, el nombre del archivo a utilizar para la operación definida. Es decir, la orden que tendremos tendrá la siguiente forma:

```
./a.out [c|d] <llave> <nombre archivo>
```

Si hemos seguido el ejemplo de compilación anterior, el ejemplo de ejecución correspondiente sería:

```
$ ./DES c holalola archivo.txt $
$ ./DES d holalola cipher_text.txt $
```

Se puede inferir que el archivo de cifrado resultante con el criptotexto de la primera llamada al programa es *cipher_text.txt*, cuyo nombre no es dinámico en ejecución, pero es muy sencillo cambiarlo en el código. Decidimos dejarlo así por claridad. Para la segunda llamada, se generará un archivo que contendrá el texto claro, resultado del descifrado. Este se podrá consultar como *plain_text.txt*, cuyo nombre también es igual para todas las entradas que proporcionemos al programa.

Posible resultado en el directorio de trabajo:

```
.
|__ cipher_text.txt
|__ DES
|__ des.c
|__ des.h
|__ plain_text.txt
```