Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Анализ программ

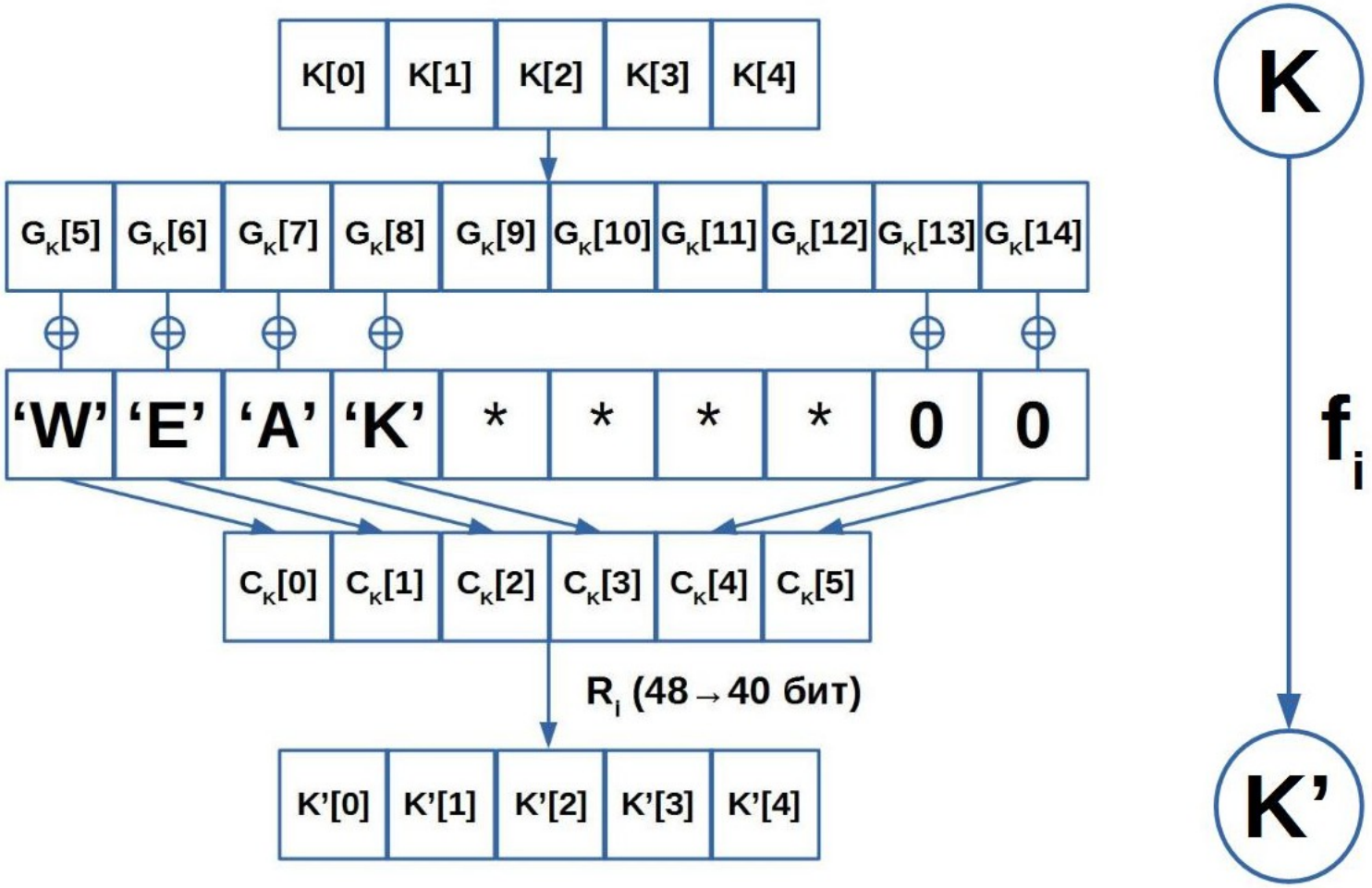
LightEditor

Формат файла:

- 4 байта - “weak”
- 8 байт – длина текста N
- N байт – текст

WeakCrypto.exe

Функция перехода



Радужные цепочки

- Количество ключей – 2^{40}
- Длина цепочки – 2^{14}
- Количество цепочек – 2^{26}
- Размер файла с цепочками – $2^{26} * 10 = 640$ Мб
- Вычислений функций перехода на поиск ключа:
  - $E(n(n-1)/2) \approx 1/2*E(n^2) = 1/2*n*(n+1)*(2n+1)/(6*n) \approx n^2/6$
  - $2^{27}/3$

Патч

C++

```
int _tmain(int argc, _TCHAR* argv[])
{
    char src[100] = "6b15ac8f", dst[100];

    __asm
    {
            pusha
            lea ecx, src
            lea edx, dst

            mov esi, 5
        label_main_loop:
            mov al, [ecx]
            cmp al, 0x39
            ja label_non_digit1
        label_digit1:
            sub al, 0x30
            jmp label_value1
        label_non_digit1:
            sub al, 0x57
        label_value1:
            shl al, 4
            inc ecx
            mov bl, [ecx]
            cmp bl, 0x39
            ja label_non_digit2
        label_digit2:
            sub bl, 0x30
            jmp label_value2
        label_non_digit2:
            sub bl, 0x57
        label_value2:
            add al, bl
            mov [edx], al
            inc ecx
            inc edx
            dec esi
            jnz label_main_loop

            popa
    }
    return 0;
}
```

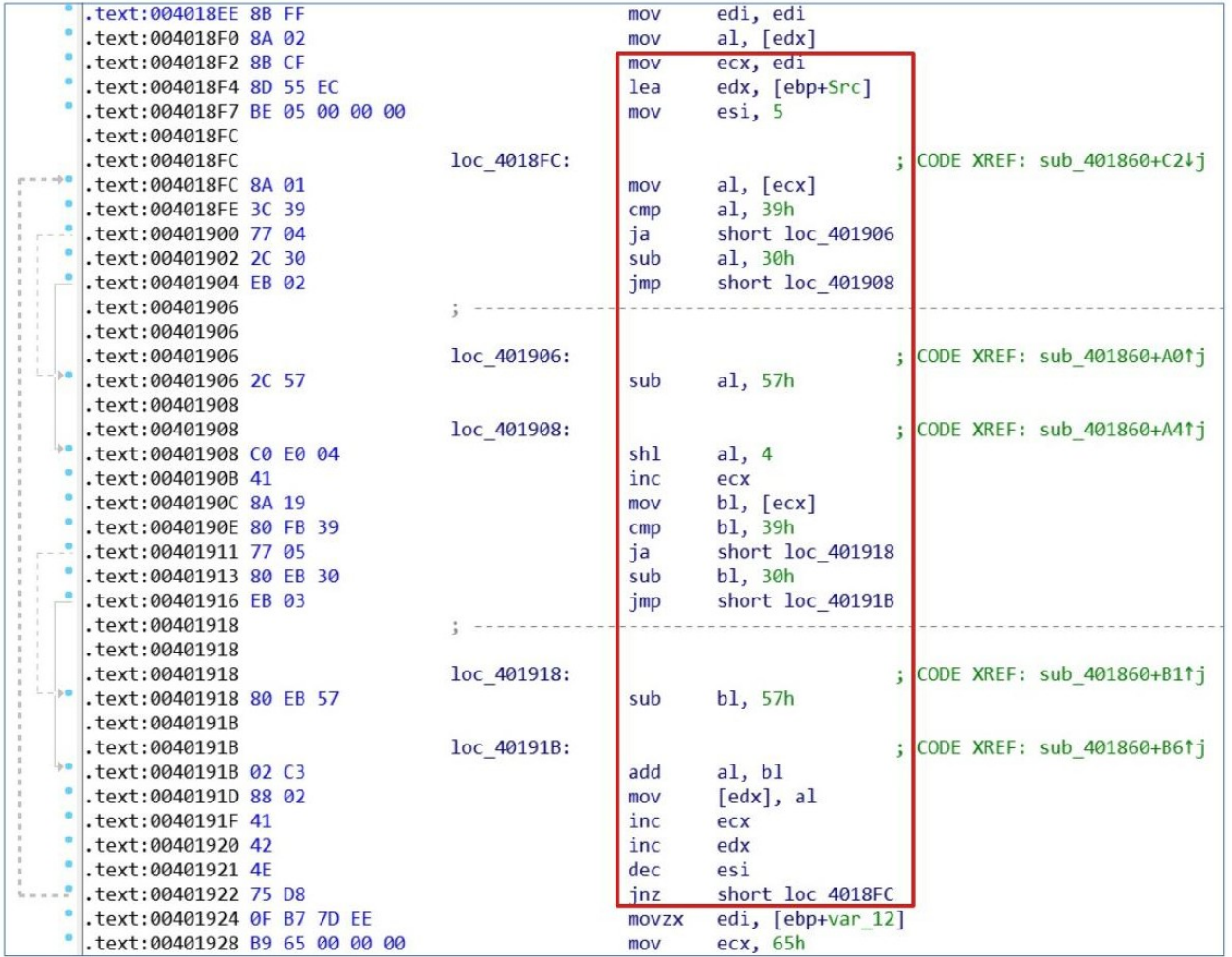
Ida

```
.text:0040102E 83 C4 0C                    add     esp, 0Ch
.text:00401031 66 60                       pushaw
.text:00401033 8D 4D 9C                    lea     ecx, [ebp+var_64]
.text:00401036 8D 95 38 FF FF FF           lea     edx, [ebp+var_C8]
.text:0040103C BE 05 00 00 00              mov     esi, 5
.text:00401041
.text:00401041                         loc_401041:                             ;
.text:00401041 8A 01                       mov     al, [ecx]
.text:00401043 3C 39                       cmp     al, 39h
.text:00401045 77 04                       ja      short loc_40104B
.text:00401047 2C 30                       sub     al, 30h
.text:00401049 EB 02                       jmp     short loc_40104D
.text:0040104B                         ; ---------------------------------------
.text:0040104B
.text:0040104B                         loc_40104B:                             ;
.text:0040104B 2C 57                       sub     al, 57h
.text:0040104D
.text:0040104D                         loc_40104D:                             ;
.text:0040104D C0 E0 04                    shl     al, 4
.text:00401050 41                          inc     ecx
.text:00401051 8A 19                       mov     bl, [ecx]
.text:00401053 80 FB 39                    cmp     bl, 39h
.text:00401056 77 05                       ja      short loc_40105D
.text:00401058 80 EB 30                    sub     bl, 30h
.text:0040105B EB 03                       jmp     short loc_401060
.text:0040105D                         ; ---------------------------------------
.text:0040105D
.text:0040105D                         loc_40105D:                             ;
.text:0040105D 80 EB 57                    sub     bl, 57h
.text:00401060
.text:00401060                         loc_401060:                             ;
.text:00401060 02 C3                       add     al, bl
.text:00401062 88 02                       mov     [edx], al
.text:00401064 41                          inc     ecx
.text:00401065 42                          inc     edx
.text:00401066 4E                          dec     esi
.text:00401067 75 D8                       jnz     short loc_401041
.text:00401069 66 61                       popaw
.text:0040106B 33 C0                       xor     eax, eax
```

Оригинальный файл

```
.text:000C18E9
.text:000C18E9                  loc_C18E9:                              ; CODE XREF: decrypt_file+67↑j
.text:000C18E9 8B D7                        mov     edx, edi
.text:000C18EB 8D 4A 01                     lea     ecx, [edx+1]
.text:000C18EE 8B FF                        mov     edi, edi
.text:000C18F0
.text:000C18F0                  loc_C18F0:                              ; CODE XREF: decrypt_file+95↓j
.text:000C18F0 8A 02                        mov     al, [edx]
.text:000C18F2 42                           inc     edx
.text:000C18F3 84 C0                        test    al, al
.text:000C18F5 75 F9                        jnz     short loc_C18F0
.text:000C18F7 2B D1                        sub     edx, ecx
.text:000C18F9 8B CF                        mov     ecx, edi        ; Src
.text:000C18FB 6A 00                        push    0               ; int
.text:000C18FD 52                           push    edx             ; Size
.text:000C18FE 8D 55 EC                     lea     edx, [ebp+Src]
.text:000C1901 E8 FA F6 FF FF               call    md5
.text:000C1906 83 C4 08                     add     esp, 8
.text:000C1909 BE 10 27 00 00               mov     esi, 2710h
.text:000C190E 8B FF                        mov     edi, edi
.text:000C1910
.text:000C1910                  loc_C1910:                              ; CODE XREF: decrypt_file+C2↓j
.text:000C1910 8D 55 EC                     lea     edx, [ebp+Src]
.text:000C1913 6A 00                        push    0               ; int
.text:000C1915 6A 10                        push    10h             ; Size
.text:000C1917 8B CA                        mov     ecx, edx        ; Src
.text:000C1919 E8 E2 F6 FF FF               call    md5
.text:000C191E 83 C4 08                     add     esp, 8
.text:000C1921 4E                           dec     esi
.text:000C1922 75 EC                        jnz     short loc_C1910
.text:000C1924 0F B7 7D EE                  movzx   edi, [ebp+var_12]
.text:000C1928 B9 65 00 00 00               mov     ecx, 65h
.text:000C192D 0F B7 45 EC                  movzx   eax, [ebp+Src]
.text:000C1931 85 FF                        test    edi, edi
.text:000C1933 0F B6 5D F0                  movzx   ebx, [ebp+var_10]
.text:000C1937 0F 44 F9                     cmovz   edi, ecx
```

Измененный файл



```
.text:004018EE 8B FF                    mov     edi, edi
.text:004018F0 8A 02                    mov     al, [edx]
.text:004018F2 8B CF                    mov     ecx, edi
.text:004018F4 8D 55 EC                 lea     edx, [ebp+Src]
.text:004018F7 BE 05 00 00 00           mov     esi, 5
.text:004018FC
.text:004018FC                  loc_4018FC:                             ; CODE XREF: sub_401860+C2↓j
.text:004018FC 8A 01                    mov     al, [ecx]
.text:004018FE 3C 39                    cmp     al, 39h
.text:00401900 77 04                    ja      short loc_401906
.text:00401902 2C 30                    sub     al, 30h
.text:00401904 EB 02                    jmp     short loc_401908
.text:00401906                  ; ---------------------------------------------------------------------------
.text:00401906
.text:00401906                  loc_401906:                             ; CODE XREF: sub_401860+A0↑j
.text:00401906 2C 57                    sub     al, 57h
.text:00401908
.text:00401908                  loc_401908:                             ; CODE XREF: sub_401860+A4↑j
.text:00401908 C0 E0 04                 shl     al, 4
.text:0040190B 41                       inc     ecx
.text:0040190C 8A 19                    mov     bl, [ecx]
.text:0040190E 80 FB 39                 cmp     bl, 39h
.text:00401911 77 05                    ja      short loc_401918
.text:00401913 80 EB 30                 sub     bl, 30h
.text:00401916 EB 03                    jmp     short loc_40191B
.text:00401918                  ; ---------------------------------------------------------------------------
.text:00401918
.text:00401918                  loc_401918:                             ; CODE XREF: sub_401860+B1↑j
.text:00401918 80 EB 57                 sub     bl, 57h
.text:0040191B
.text:0040191B                  loc_40191B:                             ; CODE XREF: sub_401860+B6↑j
.text:0040191B 02 C3                    add     al, bl
.text:0040191D 88 02                    mov     [edx], al
.text:0040191F 41                       inc     ecx
.text:00401920 42                       inc     edx
.text:00401921 4E                       dec     esi
.text:00401922 75 D8                    jnz     short loc_4018FC
.text:00401924 0F B7 7D EE              movzx   edi, [ebp+var_12]
.text:00401928 B9 65 00 00 00           mov     ecx, 65h
```

Способы защиты программ от исследования

- Обфускация кода
- Добавление кода, не влияющего на результат работы
- Шифрование надписей
- Самораспаковывающийся код
- Многопоточность
- Проверка времени исполнения программы
- Контрольная сумма для исполняемого файла

Защита программ

Внедрение защиты:

- На этапе разработки
- На этапе компиляции
- Изменение исполняемого файла

Программы защиты:

- Коммерческие – исследуются многими
- Самодельные – дорого

https://sesc-infosec.github.io/