

code -modified Keen dreams game

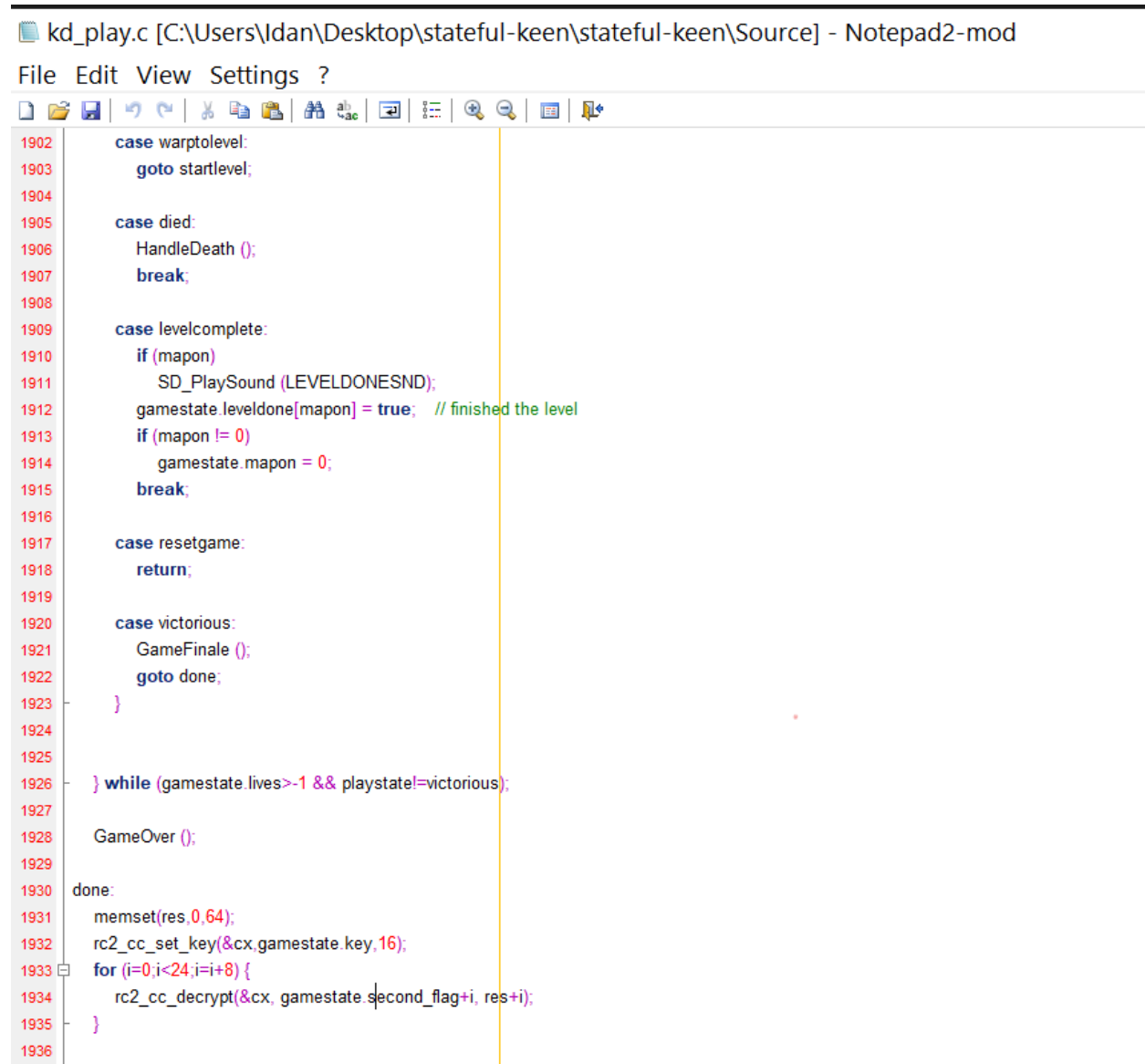
This is my direction:

id_us.c - the file where the encryption is implemented.

arr2 - probably holds the secret flag (the answer) in some form (= after encryption)

(https://github.com/search?q=rc2_cc_set_key+apple&type=Code)

They said the flag is in the source code... not sure If I need to debug



```
1902     case warptolevel:
1903         goto startlevel;
1904
1905     case died:
1906         HandleDeath ();
1907         break;
1908
1909     case levelcomplete:
1910         if (mapon)
1911             SD_PlaySound (LEVELDONESND);
1912         gamestate.leveldone[mapon] = true; // finished the level
1913         if (mapon != 0)
1914             gamestate.mapon = 0;
1915         break;
1916
1917     case resetgame:
1918         return;
1919
1920     case victorious:
1921         GameFinale ();
1922         goto done;
1923 }
1924
1925
1926 } while (gamestate.lives>-1 && playstate!=victorious);
1927
1928 GameOver ();
1929
1930 done:
1931     memset(res,0,64);
1932     rc2_cc_set_key(&cx,gamestate.key,16);
1933     for (i=0;i<24;i=i+8) {
1934         rc2_cc_decrypt(&cx, gamestate.second_flag+i, res+i);
1935     }
1936
```

kd_demo.c [C:\Users\ldan\Desktop\stateful-keen\stateful-keen\Source] - Notepad2-mod

File Edit View Settings ?

```
60 = Set up new game to start from the beginning
61 =
62 =====
63 */
64
65 void NewGame (void)
66 {
67     word i;
68
69     unsigned char arr2[24] = {0x61, 0x71, 0xf9, 0x53, 0xa6, 0x63, 0x65, 0x2, 0xc7, 0x15, 0xf0, 0x70, 0xf1, 0x95,
70         0x66, 0x1, 0x6, 0x50, 0x17, 0x35, 0x1c, 0x12, 0xc0, 0xfb};
71     gamestate.worldx = 0;    // spawn keen at starting spot
72
73     gamestate.mapon = 0;
74     gamestate.score = 0;
75     gamestate.nextextra = 20000;
76     gamestate.lives = 3;
77     gamestate.flowerpowers = gamestate.boobusbombs = 0;
78
79     memcpy(gamestate.second_flag, arr2, 24);
80     for (i = 0; i < GAMELEVELS; i++)
81         gamestate.leveldone[i] = false;
82 }
83
```

kd_demo.c [C:\Users\ldan\Desktop\stateful-keen\stateful-keen\Source] - Notepad2-mod

File Edit View Settings ?

```
60 = Set up new game to start from the beginning
61 =
62 =====
63 */
64
65 void NewGame (void)
66 {
67     word i;
68
69     unsigned char arr2[24] = {0x61, 0x71, 0xf9, 0x53, 0xa6, 0x63, 0x65, 0x2, 0xc7, 0x15, 0xf0, 0x70, 0xf1, 0x95,
70         0x66, 0x1, 0x6, 0x50, 0x17, 0x35, 0x1c, 0x12, 0xc0, 0xfb};
71     gamestate.worldx = 0;    // spawn keen at starting spot
72
73     gamestate.mapon = 0;
74     gamestate.score = 0;
75     gamestate.nextextra = 20000;
76     gamestate.lives = 3;
77     gamestate.flowerpowers = gamestate.boobusbombs = 0;
78
79     memcpy(gamestate.second_flag, arr2, 24);
80     for (i = 0; i < GAMELEVELS; i++)
81         gamestate.leveldone[i] = false;
82 }
83
```

kd_play.c [C:\Users\ldan\Desktop\stateful-keen\stateful-keen\Source] - Notepad2-mod

File Edit View Settings ?

```
1902     case warptolevel:
1903         goto startlevel;
1904
1905     case died:
1906         HandleDeath ();
1907         break;
1908
1909     case levelcomplete:
1910         if (mapon)
1911             SD_PlaySound (LEVELDONESND);
1912         gamestate.leveldone[mapon] = true; // finished the level
1913         if (mapon != 0)
1914             gamestate.mapon = 0;
1915         break;
1916
1917     case resetgame:
1918         return;
1919
1920     case victorious:
1921         GameFinale ();
1922         goto done;
1923     }
1924
1925     } while (gamestate.lives>-1 && playstate!=victorious);
1926
1927     GameOver ();
1928
1929 done:
1930     memset(res,0,64);
1931     rc2_cc_set_key(&cx,gamestate.key,16);
1932     for (i=0;i<24;i+=8) {
1933         rc2_cc_decrypt(&cx, gamestate.second_flag+i, res+i);
1934     }
1935
1936
```

בנוסף לשינויים הקודמים - אפשר לראות דיי בקלות שאת הקוד המקורי מה- [GITHUB](#) הם ערכו במקומות הבאים:

id_us_a.asm

הוסיפו פרוצדורת אסמבלי בשם

CP_RndT

וקוראים לה כאן: kd_play.c

int DoActor (objtype *ob,int tics)

אני חושב שזכור לי שספציפית על השאלה הזאת הם שמו הוראות "משחק" בעבר על כך שצריך ממש להפעיל ולשחק במשחק ומחקו את ההוראות האלו:

המערך gamestate.key מאותחל בכלל תוך כדי משחק כתלות בשלבים [וזה עוד לפני ששילבתי את הפרוצדורת אסמבלי בקוד]

(בגלל זה הם קוראים לאתגר stateful keen)

```
if (ob->state == state) {  
    if (ob==player && ob->state->choseshapenum>0 && gamestate.key_index<16) {  
        CP_InitRndT((word)ob->state->choseshapenum);  
        gamestate.key[gamestate.key_index] = CP_RndT();  
        gamestate.key_index++;  
        gamestate.key[gamestate.key_index] = CP_RndT();  
    }  
    ob->state = state->nextstate; // go to next state  
}  
else if (!ob->state)  
    return 0; // object removed itself  
return exesstics;  
}  
}
```