[Date Prev][Date Next][Thread Prev][Thread Next][Date Index][Thread Index]

Thank you Bob Anderson

- *To*: cypherpunks@toad.com
- *Subject*: Thank you Bob Anderson
- *From*: nobody@jpunix.com
- *Date*: Fri, 9 Sep 1994 22:11:49 -0500
- *Complaints-To*: postmaster@jpunix.com
- *Remailed-By*: remailer@jpunix.com
- *Sender*: owner-cypherpunks@toad.com

```
SUBJECT:  RC4 Source Code


I've tested this.  It is compatible with the RC4 object module
that comes in the various RSA toolkits.

/* rc4.h */
typedef struct rc4_key
{
     unsigned char state[256];
     unsigned char x;
     unsigned char y;
} rc4_key;
void prepare_key(unsigned char *key_data_ptr,int key_data_len,
rc4_key *key);
void rc4(unsigned char *buffer_ptr,int buffer_len,rc4_key * key);


/*rc4.c */
#include "rc4.h"
static void swap_byte(unsigned char *a, unsigned char *b);
void prepare_key(unsigned char *key_data_ptr, int key_data_len,
rc4_key *key)
{
     unsigned char swapByte;
     unsigned char index1;
     unsigned char index2;
     unsigned char* state;
     short counter;

     state = &key->state[0];
     for(counter = 0; counter < 256; counter++)
     state[counter] = counter;
     key->x = 0;
     key->y = 0;
     index1 = 0;
     index2 = 0;
     for(counter = 0; counter < 256; counter++)
     {
          index2 = (key_data_ptr[index1] + state[counter] +
index2) % 256;
          swap_byte(&state[counter], &state[index2]);

          index1 = (index1 + 1) % key_data_len;
     }
 }

 void rc4(unsigned char *buffer_ptr, int buffer_len, rc4_key
*key)
 {
    unsigned char x;
    unsigned char y;
    unsigned char* state;
    unsigned char xorIndex;
    short counter;

    x = key->x;
    y = key->y;

    state = &key->state[0];
    for(counter = 0; counter < buffer_len; counter ++)
    {
         x = (x + 1) % 256;
         y = (state[x] + y) % 256;
         swap_byte(&state[x], &state[y]);

         xorIndex = state[x] + (state[y]) % 256;

         buffer_ptr[counter] ^= state[xorIndex];
     }
     key->x = x;
     key->y = y;
}

static void swap_byte(unsigned char *a, unsigned char *b)
{
    unsigned char swapByte;

    swapByte = *a;
    *a = *b;
    *b = swapByte;
}
```

- Prev by Date: **Re: Ecash mailing list?**
- Next by Date: **Societies & Your Health**
- Prev by thread: **Copulating Camels and Digital Cash**
- Next by thread: **Re: Thank You Bob Anderson**
- Index(es):
  - **Date**
  - **Thread**