Correction to xtea

David J. Wheeler
Roger M. Needham
Computer Laboratory
Cambridge University
England

October 1998

We give below a response to the Newsgroup note on Block TEA.

The newsgroup sci.crypt.research published an effective attack on the
Block TEA code by Markku-Juhani Saarinen. We agree the attack is valid
and usage where many undetected ciphertext attacks can be made should be
rejected. The attack is effective against Block TEA, not the original TEA or
XTEA.

We have considered the lack of back propagation that was pointed out
and it seems easy to make the decoding difference propagation about as fast
as the forward coding mode. A simple and apparently safe way is detailed
below. The shifting values are different so that n=2 will not give problems.
The rearrangement makes the plus and XOR operations alternate to slightly
increase non linearity. The simple solution is about 30may be better. It has
the same simple interface as before.

Basically v[m]+= f(v[m-1]) is changed to v[m]+=f(v[m-1],v[m+1])
where m increases or decreases modulo n.

However, the re-arrangement may have introduced extra problems and
we would be pleased to hear if any are detected.

Provisional routine.

#define MX (z>>5^y<<2)+(y>>3^z<<4)^((sum^y)+(k[p&3^e]^z))

long btea( long * v, long n , long * k ) {
unsigned long z=v[n-1], y=v[0], sum=0,e,
    DELTA=0x9e3779b9 ;

long m, p, q ;
if ( n>1 ) { /* Coding Part */
    q = 6+52/n ;
    while ( q-- > 0 ) {
        sum += DELTA ;
        e = sum >> 2&3 ;
        for ( p = 0 ; p < n-1 ; p++ )
            y = v[p+1],
            z = v[p] += MX
            y = v[0] ;
            z = v[n-1] += MX
    }
    return 0 ; }
/* Decoding Part */
else if ( n < -1 ) {
    n = -n ;
    q = 6+52/n ;
    sum = q*DELTA ;
    while (sum != 0) {
        e = sum>>2 & 3 ;
        for (p = n-1 ; p > 0 ; p-- )
            z = v[p-1],
            y = v[p] -= MX
            z = v[n-1] ;
            y = v[0] -= MX
            sum -= DELTA ; }
    return 0 ; }
    return 1 ; } /* Signal n=0,1,-1 */

David Wheeler and Roger Needham email djw3@cl.cam.ac.uk rmn@cl.cam.ac.uk