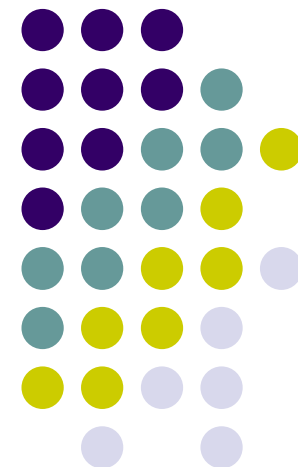


# Zcipher Algorithm

---

Ilya O. Levin

rump session @ ASIACRYPT 2007



# Zcipher: A History



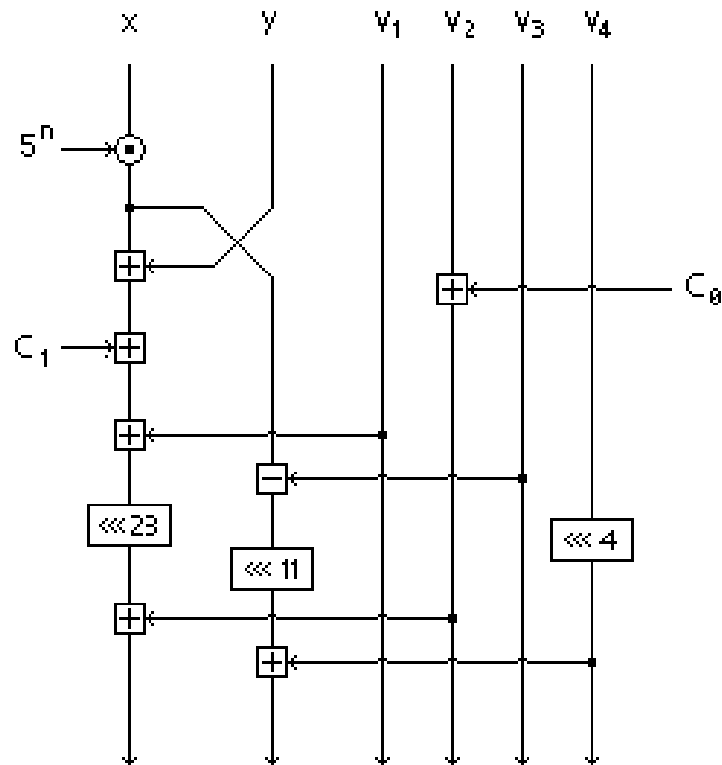
- Designed about 6 years ago as a side joke
- Surprisingly was “proprietaryized” and covered by NDA (recently lifted)
- In Nov 2007 put in public domain as a toy cipher



# Zcipher: Profile

- Simple 64-bit block cipher with 128-bit key
- Easy to understand
- Good to tease your students with or to kill another boring lunchtime

# Zcipher: Encryption



```

void encr(uint32_t *k)
{
    uint32_t t, i = ROUNDS,
             x = k[0], y = k[1],
             v1 = k[2], v2 = k[3],
             v3 = k[4], v4 = k[5];

    while (i-->0)
    {
        t = x * 0x48C27395;
        x = y + C1 + t;
        y = t;
        v2 += C0;
        v4 = R(v4, 4);
        x = R(x + v1, 23) + v2;
        y = R(y - v3, 11) + v4;
    }
    k[0] = x ^ v3; k[1] = y ^ v1;
} /* encr */

```

# Zcipher: Key Schedule



$$f(a, b, r, C) \rightarrow ((a - b) + C)_{\lll 19} + b)_{\lll r}$$

$$C_0 = 9E3779B9_{\text{hex}}$$

$$C_1 = E2E4C7C5_{\text{hex}}$$

$$C_2 = 16C7D03B_{\text{hex}}$$

$$C_3 = 3A11584F_{\text{hex}}$$

*repeat 4 times*

{

$$v_1 := f(v_2, v_1, 11, C_0)$$

$$v_2 := f(v_3, v_2, 9, C_1)$$

$$v_3 := f(v_4, v_3, 7, C_2)$$

$$v_4 := f(v_1, v_4, 10, C_3)$$

}

# Zcipher: Conclusion



More details are available at  
<http://www.literatecode.com/zcipher>

Thank you