

```
/* reverse tables */
```

```
#define RT1
V1S1,F4,A7,50) V7E,41,65,53) V7A,1,F,A4,C0) V8A,1,0,0,0,0)
V8B,AB,0B,CB) V1F,9D,4S,F1) V1AC,FA,5A,AB) V1AD,
V20,3D,FA,55) V1AD,76,6D,F0) V8A,CC,76,91) V1E,
V1F,E5,D7,FC) V1CS,2ACB,D7) V20,35,91,80) V20,
V2E,B1,5A,49) V25,BA,1B,67) V25,EA,0E,98) V25,
V3C,2F,75,02) V3E,4C,F0,12) V3D,46,97,A3) V3E,
V40,8F,5F,E7) V45,92,9C,95) V4F,6D,7A,B3) V4F,
V4D,1E,83,2D) V58,74,31,D3) V49,69,69,20) V49,
V75,C2,89,6A) V49,8E,79,78) V49,58,3E,68) V49,
V5E,B1,4F,B6) V49,8A,AD,17) V49,20,AC,06) V49,
V63,DF,4A,19) V63,1A,31,82) V63,31,2A,60) V63,
V81,64,77,E0) V81,6B,AE,84) V81,42,AB,8C) V81,
V70,48,68,58) V8F,45,FD,19) V8A,DE,6C,7E) V8A,
V1A,B,73,DX,23) V72,4B,02,E2) V81,1F,8F,57)
V81,EB,21,07) V81,B5,C2,03) V86,C,7E,91) V86,
V30,24,87,F2) V2,3,EF,A5,B2) V02,0,6A,0A) V02,
V18A,CE,1C,2B) V1A7,79,B4,92) V1,07,72,F0)
V65,DA,F4,CD) V06,05,BE,D5) V01,38,62,18)
V34,3E,53,9D) V1A,3,55,AB) V0,3A,4E,2E)
V0B,83,EC,39) V4B,66,EF,AA) V,3E,71,52,92)
V3E,71,8A,F9) V96,DD,3E,05,4E)
V91,54,AD,ES) V91,C4,07)
V19,9B,ED,94) V06,BD,E8) V1,0,0,0,0,0)
V80,E8,42,BD) V07,82,8B,82) V07,0,0,0,0,0)
V1A,7C,04,47) V7C,42,0F,E)
V09,80,86,83) V32,2B,ED,4)
VFD,0E,FF,FF) V0F,85,3E,5F) V0D,1E,05,1B)
V0A,0F,D9,64) V68,5C,A6,21) V0E,5H,4A,01)
V0C,0A,67,B1) V03,57,E7,0F) V84,EE,96,00)
V80,C0,C5,4F) V61,DC,0A,2) V5A,77,40,00)
V87,93,BA,0A) V0B,AB,2A,E5) V3C,51,ED,4)
V0E,09,0D,0E) V22,8B,C7,AD) V2D,D6,3E,8A)
V37,F1,19,85) V4F,75,07,42) V8E,39,DD,00)
V7F,01,26,8F) V0C,22,2A,0C) V4A,66,80,00)
V8B,43,29,76) VCB,43,C6,4C) V8B,ED,02,0A)
V07,31,DC,CA) V81,64,85,10) V1D,37,51,99)
V85,4A,24,7D) V2,EB,3E,F4) V1E,F9,1E,1D)
V1D,9E,3F,4B) VDC,B2,3D,F4) V8D,86,52,00)
V2D,E3,16,6C) V1A9,70,B9,99) V11,94,40,00)
V1A8,FC,8C,C4) V1A0,FD,3F,1A) V5G,70,7C,00)
V87,49,4E,C7) V09,38,D1,C1) V8C,CA,AD,00)
V1A6,F5,81,C7) V1A5,7A,DE,38) V1A4,D2,8E,00)
V2C,3A,9D,E4) V50,73,87,0D) V8A,5F,0C,00)
V86,8D,1A,C9) V90,DA,B9,E4) V8E,39,DD,00)
V8F,5D,80,8B) V89,20,8D,7D) V8F,DA,8A,00)
VCC,AC,89,3D) V10,18,7D,A7) V8E,9C,83,00)
VCD,26,78,09) V8E,59,18,F4) V8C,8A,07,00)
V8E,95,8E,65) V1A,FE,EA,7E) V1,1A,0F,00)
V8A,87,9B,D9) V1A,07,35,CB) V8A,9E,00,00)
V31,A9,82,AF) V2A,FE,31,31) V1C,AA,90,00)
V74,4E,8C,3D) V7C,81,CA,A0) V80,90,00,00)
V81,04,98,4A) V41,E0,DA,FD) V1F,0D,4E,00)
V76,4D,D6,8D) V43,6F,B0,4D) VCC,AA,90,00)
V9E,D1,85,E3) V4C,6A,84,16) V41,8F,1D,00)
V8D,8E,EA,04) V01,8C,85,5D) V1A,8F,00,00)
V83,67,1D,5A) V9D,DE,DD,5A) V8E,01,0E,00)
V9A,DD,61,80) V87,81,0C,7A) V8F,8C,7A,00)
V8C,A9,77,ED) V87,61,C9,5A) V81,1C,7A,00)
V9C,DD,DF,59) V85,F7,7A,31) V1A,1A,0F,00)
V53,F7,CD,EA) V5F,FD,AA,8B) V01,8F,00,00)
V1C,A7,F3,81) V89,68,C4,82) V38,79,00,00)
V16,1D,C3,72) V8C,E2,25,C2) V1E,AC,00,00)
V39,AS,01,71) V08,DC,B3,DE) V8B,20,7A,00)
V7B,CB,84,61) V05,32,B6,70) V8F,8C,7A,00)
```

```
#define V(a,b,c,d) 0xa1b2c3d4
static const uint32 RT1[256] =
#undef V

#define V(a,b,c,d) 0xb1c2d3e4
static const uint32 RT2[256] =
#undef V

#define V(a,b,c,d) 0xc1d2e3f4
static const uint32 RT3[256] =
#undef V

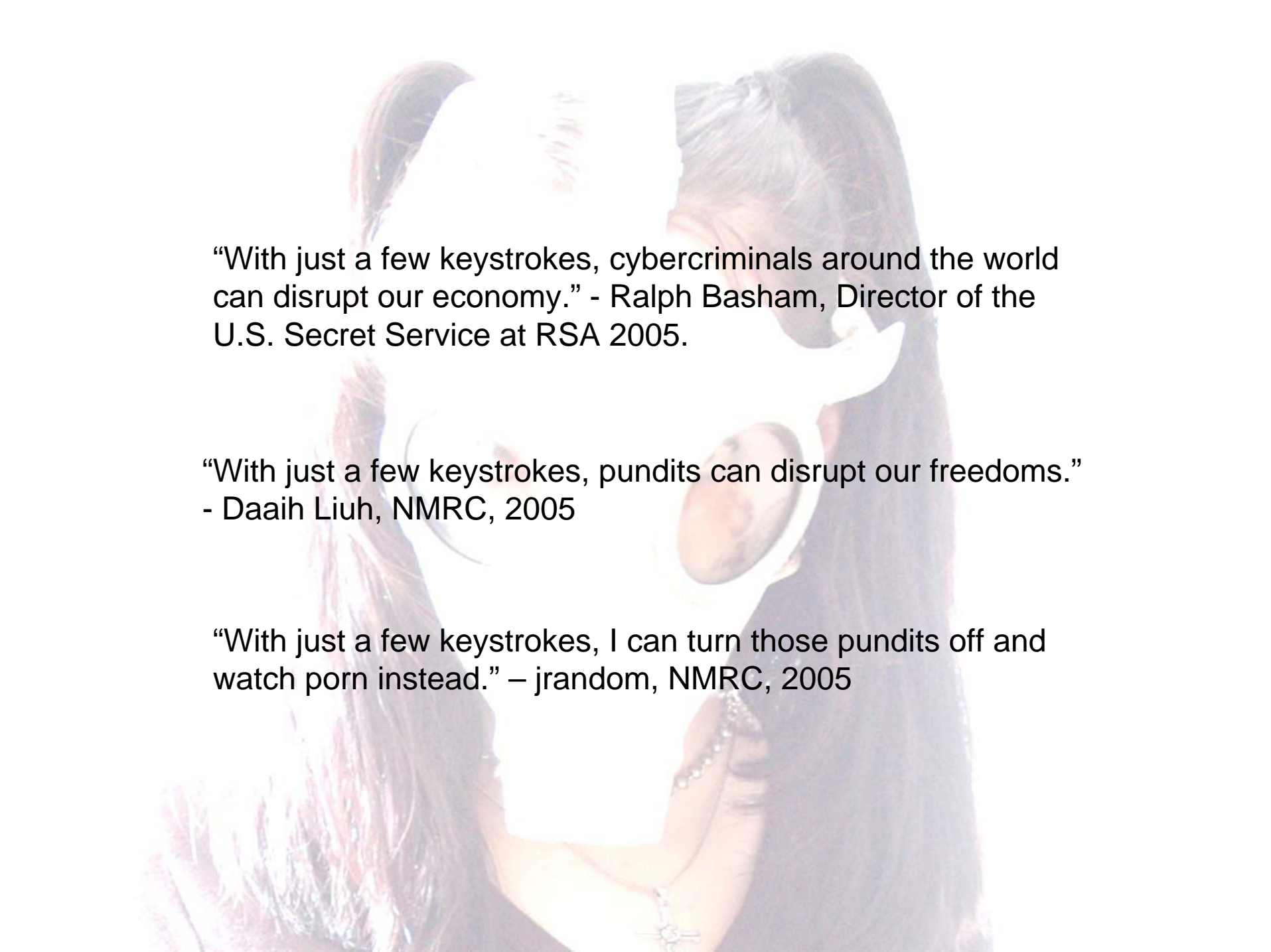
#define V(a,b,c,d) 0xd1e2f3a4
static const uint32 RT4[256] =
#undef V

/* main() */
static const uint32 RT[256] =
1
0x01000000 0x02000000 0x03000000 0x04000000
0x05000000 0x06000000 0x07000000 0x08000000
0x09000000 0x0a000000 0x0b000000 0x0c000000
0x0d000000 0x0e000000 0x0f000000 0x10000000
```

The NMRC Warez 2005 Extravaganza

DefCon 2005
nomad mobile research centre





“With just a few keystrokes, cybercriminals around the world can disrupt our economy.” - Ralph Basham, Director of the U.S. Secret Service at RSA 2005.

“With just a few keystrokes, pundits can disrupt our freedoms.”
- Daaih Liuh, NMRC, 2005

“With just a few keystrokes, I can turn those pundits off and watch porn instead.” – jrandom, NMRC, 2005

Who We Are



```
/* reverse tables */
```

```

#define RT1
V151.F4.A7.50) V17E.41.65.53) V1A.1.F.A4.C0) V1B0.
V1B8.AB.0B.CE) V1F.9D.45.F1) V1AC.FA.5A.A6) V1D0.
V1D4.30.FA.55) V1AD.76.6D.F0) V1B8.CC.76.91) V1E0.
V1F.E5.D7.FC) V1CS.2.ACB.D7) V1Q.6.35.41.80) V1R0.
V1DE.B1.5A.49) V1D5.BA.1B.67) V1F5.EA.0E.96) V1G0.
V1K3.2F.75.02) V1B1.4C.F0.12) V1B0.46.97.A3) V1C0.
V1Q3.8F.5F.E7) V1S.92.9C.95) V1BF.6D.7A.B3) V1E0.
V1D1.BE.83.2D) V1S8.74.31.D3) V1A9.E0.69.20) V1E0.
V175.C3.49.6A) V1F4.8E.79.70) V1A9.58.3E.6B) V1F0.
V1EB.E1.4F.B6) V1F0.8A.AD.17) V1CS.2.0AC.06) V1E0.
V163.DF.4A.19) V1CS.1A.31.82) V1B5.51.2A.60) V1E0.
V1B1.64.77.E0) V1B1.6B.AE.84) V1E.42.A0.4E) V1E0.
V170.48.68.58) V1BF.45.FD.19) V1B4.0E.6C.7A) V1E0.
V1AB.73.DX.2.3) V1Z.4B.02.E2) V1E3.1F.BF.57) V1E0.
V1E3.EB.21.07) V1F.B5.C2.03) V1B6.C7.1B.9E) V1E0.
V130.24.87.F2) V1Z.EF.A5.B2) V1O2.0.6A.0A) V1E0.
V1B.A.CE.1C.2B) V1A7.79.B4.92) V1E.07.72.F7) V1E0.
V165.DA.F4.CD) V1O6.05.BE.D5) V1D1.48.62.18) V1E0.
V134.3E.53.9D) V1A2.F3.55.A0) V1B5.4A.E1.72) V1E0.
V1B8.83.EC.39) V1B0.60.EF.AA) V15E.71.97.06) V1E0.
V1B6.71.8A.F9) V1F6.DD.06.8D) V1D0.4B.05.AE) V1E0.
V191.54.1D.E5) V1F1.C4.3D.03) V1B4.66.04.82) V1E0.
V112.9B.FD.24) V1D6.BDE.97.97) V1B5.40.82.2E) V1E0.
V1B0.E8.42.BD) V1Q7.82.8B.80) V1E7.19.4E.49) V1E0.
V1A1.7C.04.47) V17C.42.0F.E9) V1E8.74.1E.C0) V1E0.
V109.80.86.83) V132.21.ED.40) V1FE.11.70.42) V1E0.
V1FD.0E.FF.F0) V1Q7.85.3E.56) V1D1.AE.D5.1B) V1E0.
V10A.0F.D9.64) V168.5C.A6.21) V1B5.51.4A.01) V1E0.
V10C.0A.67.B1) V1Q3.57.E7.0F) V1B4.EE.96.00) V1E0.
V1B0.C0.C5.4F) V1G1.DC.0.A2) V1BA.F7.40.99) V1E0.
V1E7.93.BA.0A) V1C0.A0.2A.E5) V13C.51.E0.41) V1E0.
V10E.09.0D.0B) V1F2.4B.C7.AD) V1ZD.D6.4E.80) V1E0.
V1G7.F1.19.85) V1AF.75.07.4C) V1E2.39.D0.30) V1E0.
V1F7.01.26.8F) V1CC.22.FA.C3) V144.66.80.C5) V1E0.
V1B8.43.29.76) V1CB.23.C6.4C) V1B0.E0.F0.0A) V1E0.
V1D7.31.DC.CA) V1B2.63.85.10) V1D1.37.5A.99) V1E0.
V185.4A.24.7D) V1Z2.BB.3B.F4) V1AE.F9.81.01) V1E0.
V1D1.9E.2F.4B) V1DC.B2.30.F4) V1D0.86.52.2C) V1E0.
V1D2.E3.16.6C) V1A9.7D.B9.94) V1B5.40.82.2E) V1E0.
V1A8.FC.8C.C4) V1A0.F0.3F.1E) V18C.C0.00.00) V1E0.
V1B7.49.4E.C7) V1D9.38.D1.C4) V18C.C0.00.00) V1E0.
V1A6.F5.81.CF) V1A5.7A.1E.31) V144.66.80.C5) V1E0.
V1C6.3A.9D.E4) V150.78.97.0A) V1B4.51.8A.5D) V1E0.
V1F6.8D.1A.C9) V1F0.D4.1B.E4) V1E0.
V1F9.5D.80.BB) V1B9.70.10.F7) V1E0.
V1C5.AE.89.3D) V110.1B.D1.A4) V1E0.
V1CD.26.78.09) V1E6.59.18.F4) V1E3.8A.D5.0E) V1E0.
V1E6.95.6E.65) V1AA.F1.E6.7E) V1D1.AE.D5.1B) V1E0.
V1BA.E7.9B.D9) V1A4.07.3B.CB) V1E3.8A.D5.0E) V1E0.
V131.A9.E2.A7) V1D4.1E.73.31) V1C6.A1.9E.0E) V1E0.
V174.4E.BC.3D) V1FC.81.CA.A0) V1B0.90.0E.0E) V1E0.
V1F1.04.98.4A) V141.EC.DA.FD) V1FF.CD.4A.0E) V1E0.
V176.4D.D6.8D) V143.EF.B0.4D) V1CC.AA.4A.4A) V1E0.
V19E.D1.B5.E3) V1FC.6.A.84.1B) V1C1.N.17.0E) V1E0.
V1B0.SE.EA.04) V171.8C.35.5D) V1A.A.E7.9B.D9) V1E0.
V1B3.67.1D.5A) V191.DE.D0.5A) V1E0.16.6C) V1E0.
V19A.D7.C1.8A) V1Z7.A1.0C.7A) V1F0.4C.7A.8E) V1E0.
V1C5.A9.77.EB) V1B7.61.C9.5A) V1B1.67.0E.0E) V1E0.
V19C.DD.DF.59) V155.F7.7A.31) V1A1.1E.8E.0E) V1E0.
V153.F7.CD.EA) V15F.FD.A1.2B) V1D1.37.5A.99) V1E0.
V1CA.A7.F7.81) V1B9.68.C4.82) V130.24.87.F2) V1E0.
V161.DC.72) V1E0.E2.25.C7) V1E2.39.D0.30) V1E0.
V139.A8.01.71) V10E.DC.B3.DE) V1B8.20.1F.0E) V1E0.
V17B.CB.84.64) V1D5.32.E6.70) V1A0.70.3F.1E) V1E0.

```

```

#define V(a,b,c,d) 0x10000000
static const uint32 RT1[] = {
    #undef V
}

#define V(a,b,c,d) 0x20000000
static const uint32 RT2[] = {
    #undef V
}

#define V(a,b,c,d) 0x30000000
static const uint32 RT3[] = {
    #undef V
}

#define V(a,b,c,d) 0x40000000
static const uint32 RT4[] = {
    #undef V
}

#define V(a,b,c,d) 0x50000000
static const uint32 RT5[] = {
    #undef V
}

#define V(a,b,c,d) 0x60000000
static const uint32 RT6[] = {
    #undef V
}

#define V(a,b,c,d) 0x70000000
static const uint32 RT7[] = {
    #undef V
}

#define V(a,b,c,d) 0x80000000
static const uint32 RT8[] = {
    #undef V
}

#define V(a,b,c,d) 0x90000000
static const uint32 RT9[] = {
    #undef V
}

#define V(a,b,c,d) 0xA0000000
static const uint32 RT10[] = {
    #undef V
}

#define V(a,b,c,d) 0xB0000000
static const uint32 RT11[] = {
    #undef V
}

#define V(a,b,c,d) 0xC0000000
static const uint32 RT12[] = {
    #undef V
}

#define V(a,b,c,d) 0xD0000000
static const uint32 RT13[] = {
    #undef V
}

#define V(a,b,c,d) 0xE0000000
static const uint32 RT14[] = {
    #undef V
}

#define V(a,b,c,d) 0xF0000000
static const uint32 RT15[] = {
    #undef V
}

#define V(a,b,c,d) 0x00000000
static const uint32 RT16[] = {
    #undef V
}

#define V(a,b,c,d) 0x10000000
static const uint32 RT17[] = {
    #undef V
}

#define V(a,b,c,d) 0x20000000
static const uint32 RT18[] = {
    #undef V
}

#define V(a,b,c,d) 0x30000000
static const uint32 RT19[] = {
    #undef V
}

#define V(a,b,c,d) 0x40000000
static const uint32 RT20[] = {
    #undef V
}

#define V(a,b,c,d) 0x50000000
static const uint32 RT21[] = {
    #undef V
}

#define V(a,b,c,d) 0x60000000
static const uint32 RT22[] = {
    #undef V
}

#define V(a,b,c,d) 0x70000000
static const uint32 RT23[] = {
    #undef V
}

#define V(a,b,c,d) 0x80000000
static const uint32 RT24[] = {
    #undef V
}

#define V(a,b,c,d) 0x90000000
static const uint32 RT25[] = {
    #undef V
}

#define V(a,b,c,d) 0xA0000000
static const uint32 RT26[] = {
    #undef V
}

#define V(a,b,c,d) 0xB0000000
static const uint32 RT27[] = {
    #undef V
}

#define V(a,b,c,d) 0xC0000000
static const uint32 RT28[] = {
    #undef V
}

#define V(a,b,c,d) 0xD0000000
static const uint32 RT29[] = {
    #undef V
}

#define V(a,b,c,d) 0xE0000000
static const uint32 RT30[] = {
    #undef V
}

#define V(a,b,c,d) 0xF0000000
static const uint32 RT31[] = {
    #undef V
}

#define V(a,b,c,d) 0x00000000
static const uint32 RT32[] = {
    #undef V
}

#define V(a,b,c,d) 0x10000000
static const uint32 RT33[] = {
    #undef V
}

#define V(a,b,c,d) 0x20000000
static const uint32 RT34[] = {
    #undef V
}

#define V(a,b,c,d) 0x30000000
static const uint32 RT35[] = {
    #undef V
}

#define V(a,b,c,d) 0x40000000
static const uint32 RT36[] = {
    #undef V
}

#define V(a,b,c,d) 0x50000000
static const uint32 RT37[] = {
    #undef V
}

#define V(a,b,c,d) 0x60000000
static const uint32 RT38[] = {
    #undef V
}

#define V(a,b,c,d) 0x70000000
static const uint32 RT39[] = {
    #undef V
}

#define V(a,b,c,d) 0x80000000
static const uint32 RT40[] = {
    #undef V
}

#define V(a,b,c,d) 0x90000000
static const uint32 RT41[] = {
    #undef V
}

#define V(a,b,c,d) 0xA0000000
static const uint32 RT42[] = {
    #undef V
}

#define V(a,b,c,d) 0xB0000000
static const uint32 RT43[] = {
    #undef V
}

#define V(a,b,c,d) 0xC0000000
static const uint32 RT44[] = {
    #undef V
}

#define V(a,b,c,d) 0xD0000000
static const uint32 RT45[] = {
    #undef V
}

#define V(a,b,c,d) 0xE0000000
static const uint32 RT46[] = {
    #undef V
}

#define V(a,b,c,d) 0xF0000000
static const uint32 RT47[] = {
    #undef V
}

#define V(a,b,c,d) 0x00000000
static const uint32 RT48[] = {
    #undef V
}

#define V(a,b,c,d) 0x10000000
static const uint32 RT49[] = {
    #undef V
}

#define V(a,b,c,d) 0x20000000
static const uint32 RT50[] = {
    #undef V
}

#define V(a,b,c,d) 0x30000000
static const uint32 RT51[] = {
    #undef V
}

#define V(a,b,c,d) 0x40000000
static const uint32 RT52[] = {
    #undef V
}

#define V(a,b,c,d) 0x50000000
static const uint32 RT53[] = {
    #undef V
}

#define V(a,b,c,d) 0x60000000
static const uint32 RT54[] = {
    #undef V
}

#define V(a,b,c,d) 0x70000000
static const uint32 RT55[] = {
    #undef V
}

#define V(a,b,c,d) 0x80000000
static const uint32 RT56[] = {
    #undef V
}

#define V(a,b,c,d) 0x90000000
static const uint32 RT57[] = {
    #undef V
}

#define V(a,b,c,d) 0xA0000000
static const uint32 RT58[] = {
    #undef V
}

#define V(a,b,c,d) 0xB0000000
static const uint32 RT59[] = {
    #undef V
}

#define V(a,b,c,d) 0xC0000000
static const uint32 RT60[] = {
    #undef V
}

#define V(a,b,c,d) 0xD0000000
static const uint32 RT61[] = {
    #undef V
}

#define V(a,b,c,d) 0xE0000000
static const uint32 RT62[] = {
    #undef V
}

#define V(a,b,c,d) 0xF0000000
static const uint32 RT63[] = {
    #undef V
}

#define V(a,b,c,d) 0x00000000
static const uint32 RT64[] = {
    #undef V
}

```

On To The Warez....



Updated Ncrypt

- New features and bug fixes
 - Includes Todd MacDermind's nrm, a drop-in replacement for rm for secure file erasure
 - More features for script integration (the users demanded it!)

Stronghold

- For Windows 2000, XP, 2003
- Locks down the box
 - Implements the NIST standards for securing Windows
- Rollback feature
- GPL, and it's freeware, feel the love

Stronghold Analyzer

- For Windows 2000, XP, 2003
- Like Stronghold, it uses NIST standards for securing Windows
- Shows security holes that exist in Windows that Stronghold will secure
- GPL, and it's freeware, feel even more love

Stronghold / Stronghold Analyzer Demo



SPA

- SPA is Single Packet Authentication, a single packet that can authenticate a user to a system
- It is a protocol for allowing a remote user to authenticate securely on a “closed” system (limited or no open services)
- Uses GPG to sign/encrypt a message to a sniffing server in a single TCP, UDP, or ICMP packet
- Work across NAT
- Free

SPA Demo



NPC

- NPC is Nearly Perfect Crypto. Seriously....
- It includes a utility for creating large one time pads (using the PRNG ISAAC)
- Fast, simple and quick
- If you can manage the key exchange, it is nearly the most perfect and unbreakable crypto you can get (one time pads are considered the ultimate crypto)
 - Key management is a bitch, and may render this impractical for modern humans

NPC Demo



Q & A

- We will spank audience members during the Q & A
- You must sign our Ass Release Form before you can be spanked
- You may choose any NMRC member to spank you
- If you do not choose a particular NMRC hacker to spank you, the NMRC hacker answering the question will spank you while giving the answer





FIN, Biatchez

Images © 2005 NMRC
www.nmrc.org