New Cryptanalysis of an Old Block Cipher

Adam Suhl[1] Peter Schmidt-Nielsen[2]

[1]UC San Diego

[2]Redwood Research

August 16, 2022

Triple-ROT13 is Broken in 3 Seconds on a Laptop

Adam Suhl[1] Peter Schmidt-Nielsen[2]

[1]UC San Diego

[2]Redwood Research

August 16, 2022

History

History

ROT13 sound design, but 0-bit keysize too small

History

ROT13 sound design, but 0-bit keysize too small

2ROT13 vulnerable to meet-in-the-middle

History

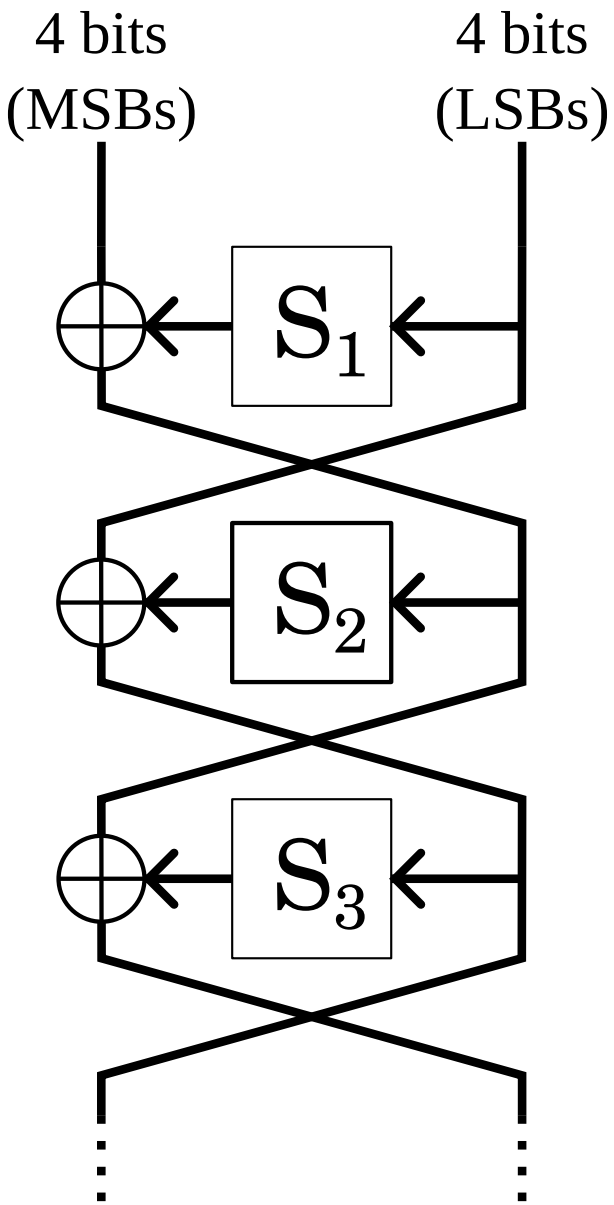
ROT13 sound design, but 0-bit keysize too small

2ROT13 vulnerable to meet-in-the-middle

3ROT13 twice as many bits of security as ROT13 (namely, zero)

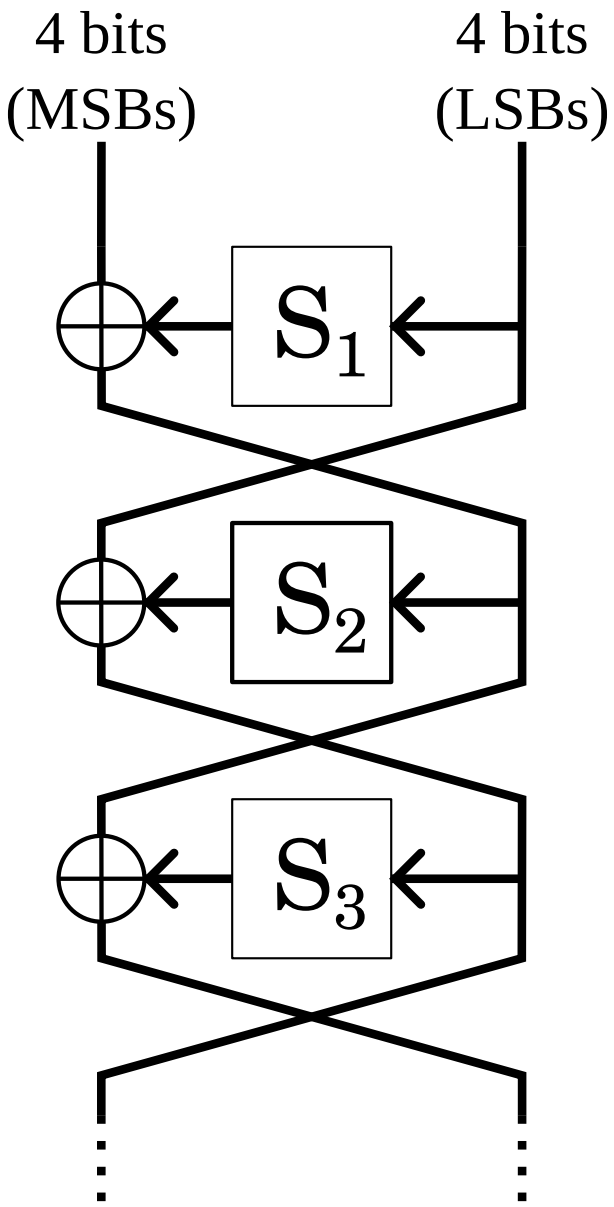
ROT13 Internals

ROT13 Internals



- Ordinary Feistel cipher
- 8-bit blocksize, 0-bit keysize
- 6 round functions (each just a 4-bit S-box)
- Iterate these 6 Feistel rounds 13 times for ROT13
- Total: 78 rounds for ROT13, 234 rounds for 3ROT13

ROT13 Internals



- Ordinary Feistel cipher
- 8-bit blocksize, 0-bit keysize
- 6 round functions (each just a 4-bit S-box)
- Iterate these 6 Feistel rounds 13 times for ROT13
- Total: 78 rounds for ROT13, 234 rounds for 3ROT13

S-boxes

```
S1 = 08054c9108d54d81
S2 = c9c97a7adada0909
S3 = 0d9ddcdc0d9dd9d0
S4 = bdbd8f8f8585bebe
S5 = d8d54c9108d55c90
S6 = 222222200000000
```

Differential Characteristic

Differential Characteristic

$$\Pr\left[3\mathrm{ROT13}(m \oplus \texttt{0x20}) = 3\mathrm{ROT13}(m) \oplus \texttt{0x20}\right] = 1$$

Differential Characteristic

Differential Characteristic

$$\Pr\left[3\mathrm{ROT13}(m \oplus \texttt{0x20}) = 3\mathrm{ROT13}(m) \oplus \texttt{0x20}\right] = 1$$

Holds for all 234 rounds of 3ROT13!

Time for a “live” demo!

```
eve@mitm$ time python z3rot13.py
```

```
eve@mitm$ time python z3rot13.py
Ciphertext:
-----BEGIN 3ROT13 MESSAGE-----
Jr hfr vaqhfgel-fgnaqneq FFY 3.0 sbe qngn-va-genafvg
naq zvyvgnel-tenqr gevcyr-EBG13 sbe qngn-ng-erfg.
Lbhe frpergf ner fnsr jvgu hf!
-----END 3ROT13 MESSAGE-----
Plaintext:
```

```
eve@mitm$ time python z3rot13.py
Ciphertext:
-----BEGIN 3ROT13 MESSAGE-----
Jr hfr vaqhfgel-fgnaqneq FFY 3.0 sbe qngn-va-genafvg
naq zvyvgnel-tenqr gevcyr-EBG13 sbe qngn-ng-erfg.
Lbhe frpergf ner fnsr jvgu hf!
-----END 3ROT13 MESSAGE-----
Plaintext:
-----ORTVA 3EBG13 ZRFFNTR-----
We use industry-standard SSL 3.0 for data-in-transit
and military-grade triple-ROT13 for data-at-rest.
Your secrets are safe with us!
-----RAQ 3EBG13 ZRFFNTR-----

real 0m3.358s
user 0m3.302s
sys 0m0.044s
eve@mitm$
```

What now?

- 3ROT13 is dead
- Need to make an Advanced Rotation Standard
- Alternatively: destroy all laptops