Intentionally Temporarily Insecure

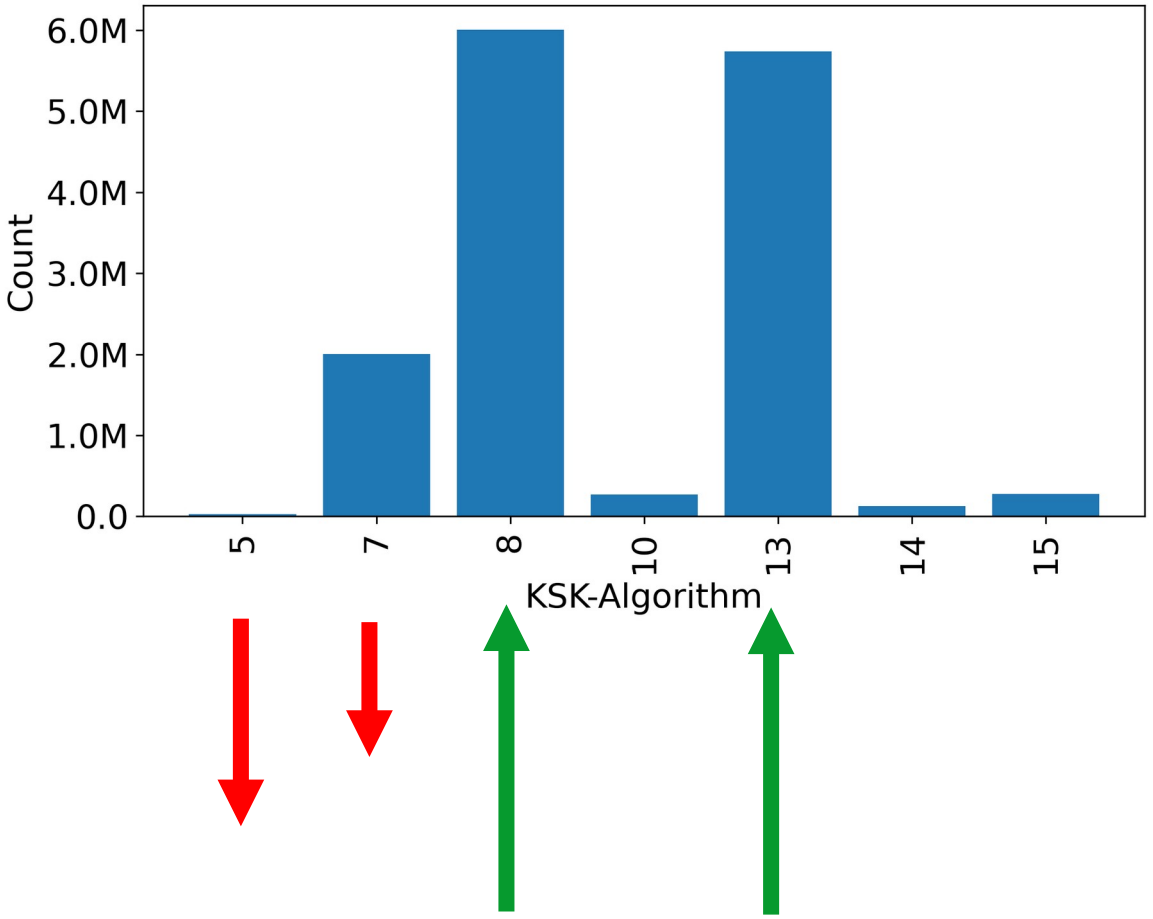
the cheater's guide to algorithm rolls

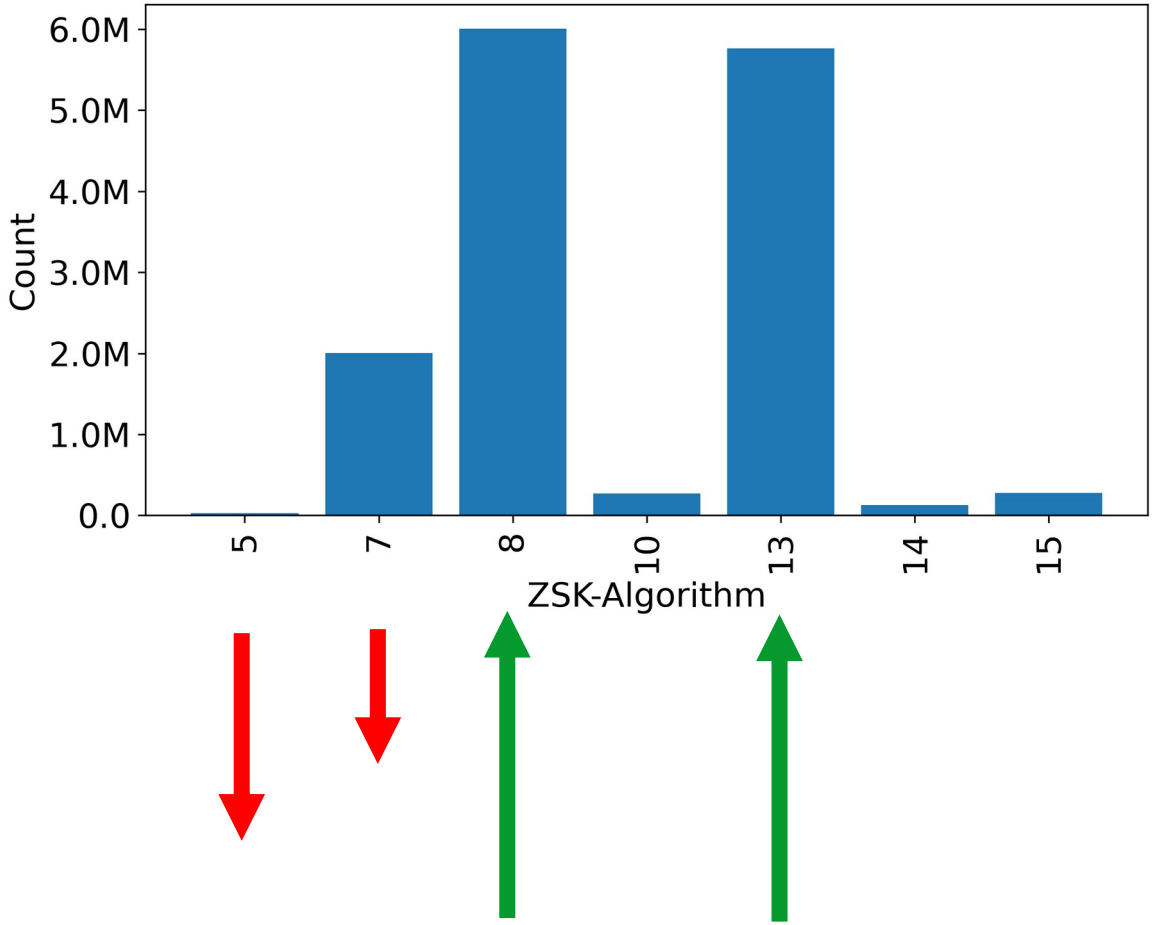
Wes Hardaker
<hardaker@isi.edu>

Algorithm Assignments and Software Recommendations

Algorithm Number	Algorithm	RFC8624 Signing Recommendation
1	RSA/MD5	• MUST NOT
5	RSA/SHA1	• NOT RECOMMENDED
7	RSA/SHA1 w/ NSEC3	• NOT RECOMMENDED
8	RSA/SHA256	• MUST
10	RSA/SHA512	• NOT RECOMMENDED
12	GOST R 34.10-2001	• MUST NOT
13	ECDSA Curve P-256 with SHA-256	• MUST
14	ECDSA Curve P-384 with SHA-384	• MAY
15	Ed25519	• RECOMMENDED
16	Ed448	• MAY

Current DNSSEC algorithm popularities

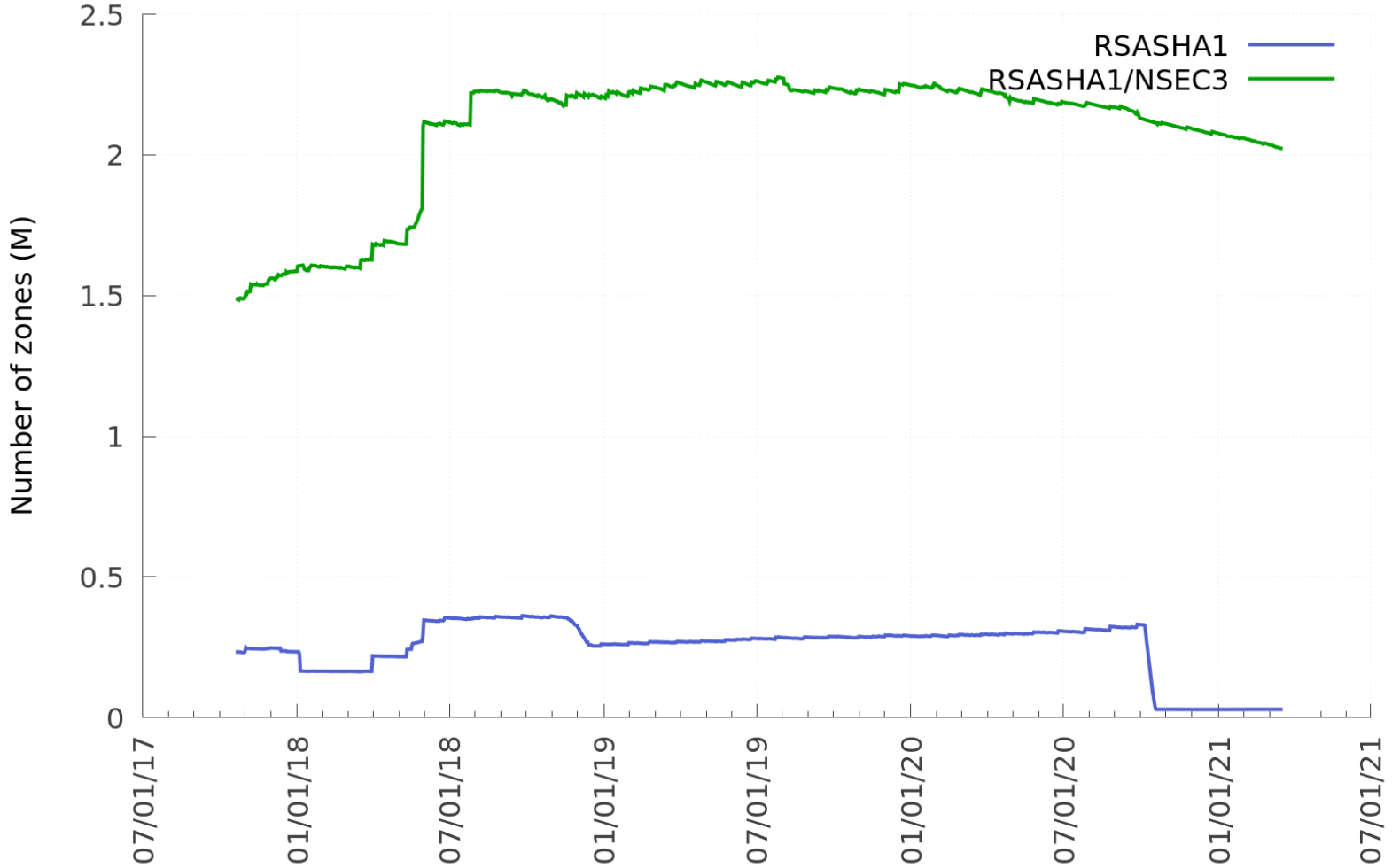




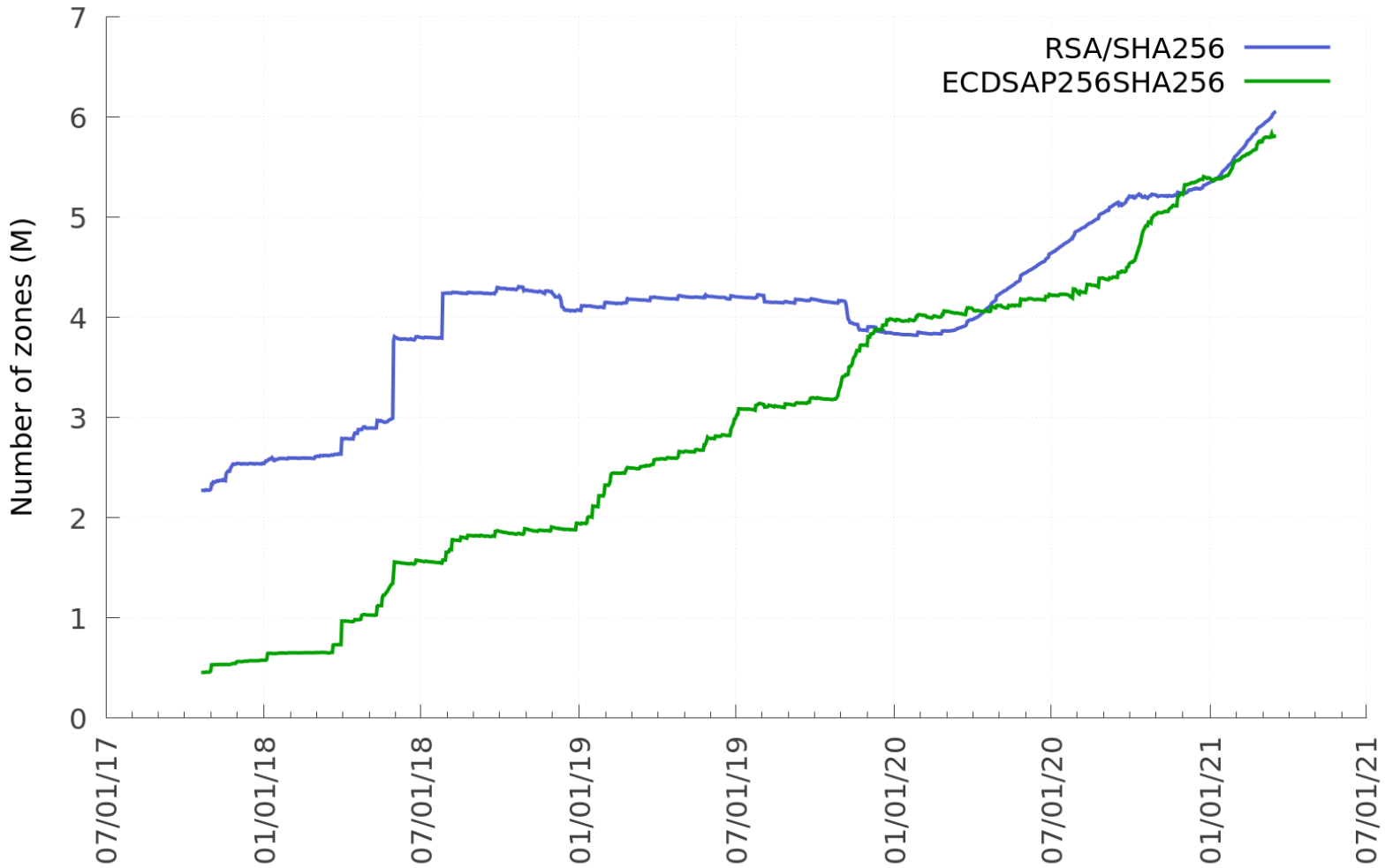
(and you should too)

The fall of the older algorithms

- RSASHA1 is beyond “decline”
- RSASHA1/NSEC3 is declining



The fall of the older algorithms



Current popular algorithms:

- RSA/SHA256 (8)
- ECDSA P-256 SHA256 (13)

Algorithm Recommendations

- If you're starting a new zone today:
  - Pick algorithm RSA/SHA256 (8) or ECDSA P-256 SHA256 (13)
  - Note: signature sizes of RSA/SHA256 are larger than the ECDSA algorithm
- If you're still using RSA-SHA1 or RSA-SHA1/NSEC3:
  - It's time to switch to RSA/SHA256 (8) or ECDSA P-256 SHA256 (13)

- But… how?

The Right Way – RFC6781 Section 4.1.4

1) Create the new DNSKEYs with the new algorithm *(both KSK and ZSK)*
   - **BUT DON'T PUBLISH IT!!**
2) Sign the zone with both the old DNSKEYs and new DNSKEYs
   - **BUT FOR THE NEW DNSKEY PUBLISH ONLY THE RRSIGs, not the DNKSEY itself**
   - Wait … for a RRSIG TTL length *(really: 2x TTL for safety)*
3) Publish the zone with a new DNSKEYs
   - Wait for a RRSIG TTL length
4) Publish the new DS record and remove the old DS record in the parent
   - Wait for a DS TTL length
5) Remove the old DNSKEYs from the zone
   - Wait for a RRSIG TTL length
6) Remove the old DNKSEYs RRSIGs

The Wrong But Acceptable Way – Cheat!

1) Remove all DS records from the parent — **You'll be "insecure"**
2) Wait for DS TTL seconds
3) Replace the old DNSKEYs with your new ones
4) Wait for the zone's negative cache time
5) Add the new DS record to the parent — **You're now secure again**

Optionally: reduce your TTLs before performing these steps

(its typically not possible to reduce the parent's DS TTL though)

Comparisons

- Pros/Cons
  - **PRO**: “cheating” is operationally much simpler
  - **PRO:** Less prone to human mistakes
  - **CON:** temporarily transitions the zone out of DNSSEC protection

- When should you consider cheating?
  - When you are **not using a automated DNSSEC software** suite that does this for you
  - When you are more concerned about stability vs security
    - What’s your threat model?

- When should you update to newer algorithms?
  - Now

Questions?