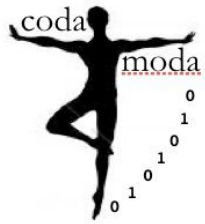
The Rupture API: Productizing TLS attacks

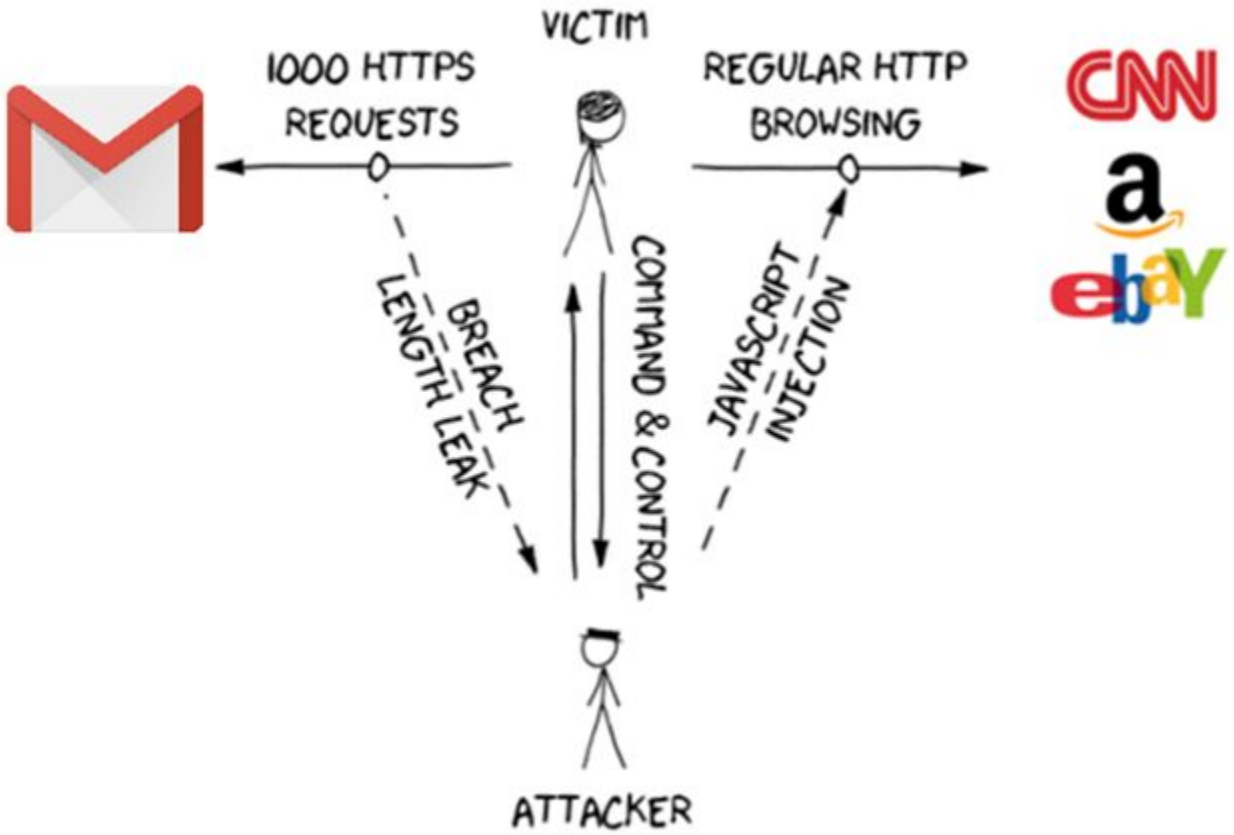
Aggelos Kiayias
Eva Sarafianou
Dionysis Zindros

Real World Crypto 2017

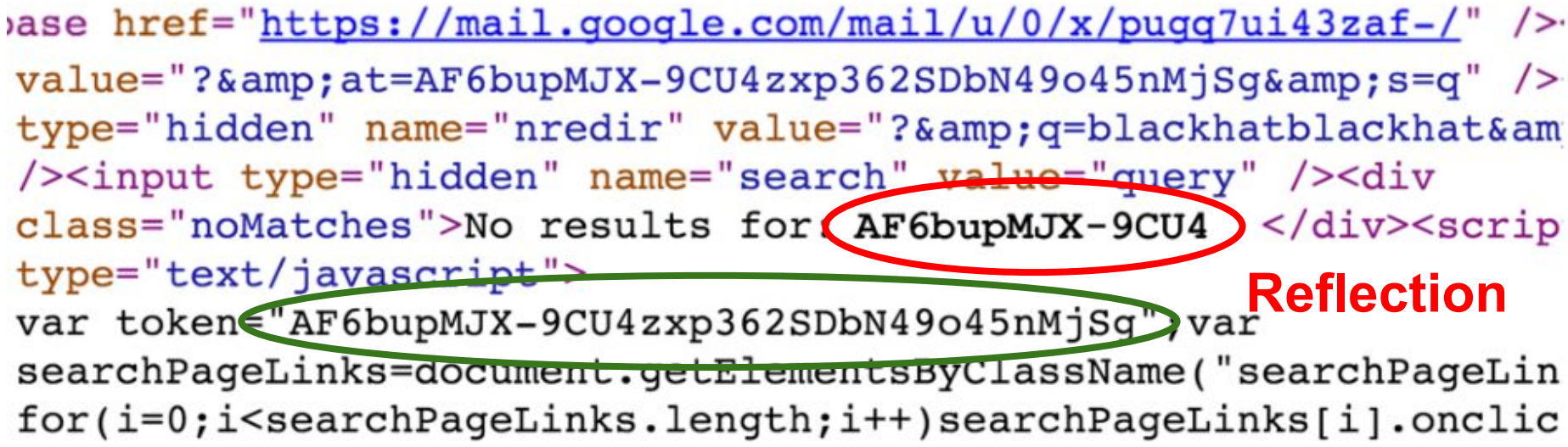
Panoramix



Attack Anatomy



- Attacker **guesses part of secret**
- Uses it in **reflection**
- Compressed/encrypted response **is shorter** if right!

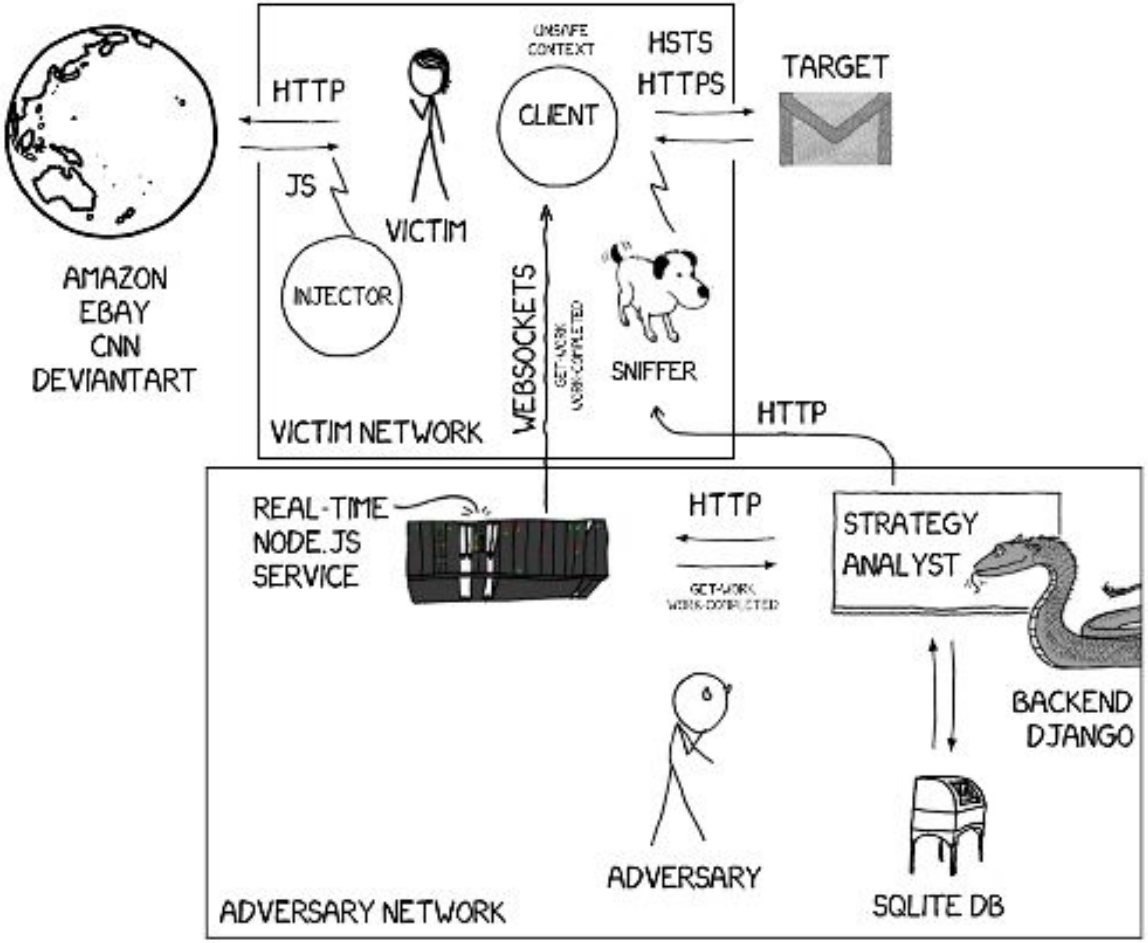


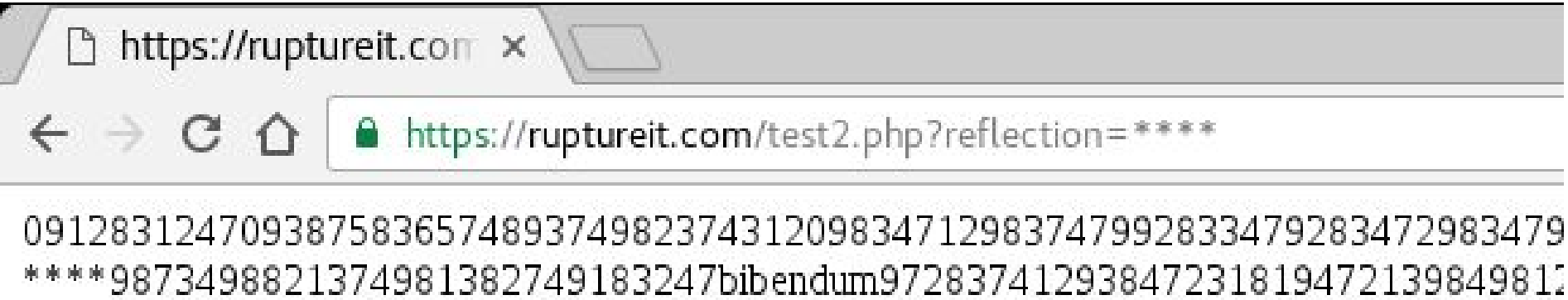
Adaptively choosing reflections strings can lead to **full recovery.**

But there are challenges:

1. Noise
2. Antagonistic compression methods (Huffman coding)
3. Unrelated static content on page matching candidates

RUPTURE ARCHITECTURE




https://ruptureit.com
https://ruptureit.com/test2.php?reflection=****
0912831247093875836574893749823743120983471298374799283347928347298347 9
****98734988213749813827491832 47bibendum9728374129384723181947213984981 2

Our Contributions

- **Usable** open-source tool
- Demonstrate attack is **easy** and **practical** via web UI
- Reusable **RESTful API**

Demo

Rupture

localhost:3000

Network Overview

Completed

Running & Paused

Not started

Scan for victims

Add custom victim

Rupture

localhost:3000

Network Overview

Completed

Running & Paused

Not started

Scan for victims

Add custom victim

Rupture

localhost:3000

Network Overview

Completed

Running & Paused

Not started

Scanning...

Add custom victim

RuptureIt

Rupture

localhost:3000

Network Overview

Completed

Running & Paused

Not started

Not started
192.168.1.1

Not started
192.168.1.2

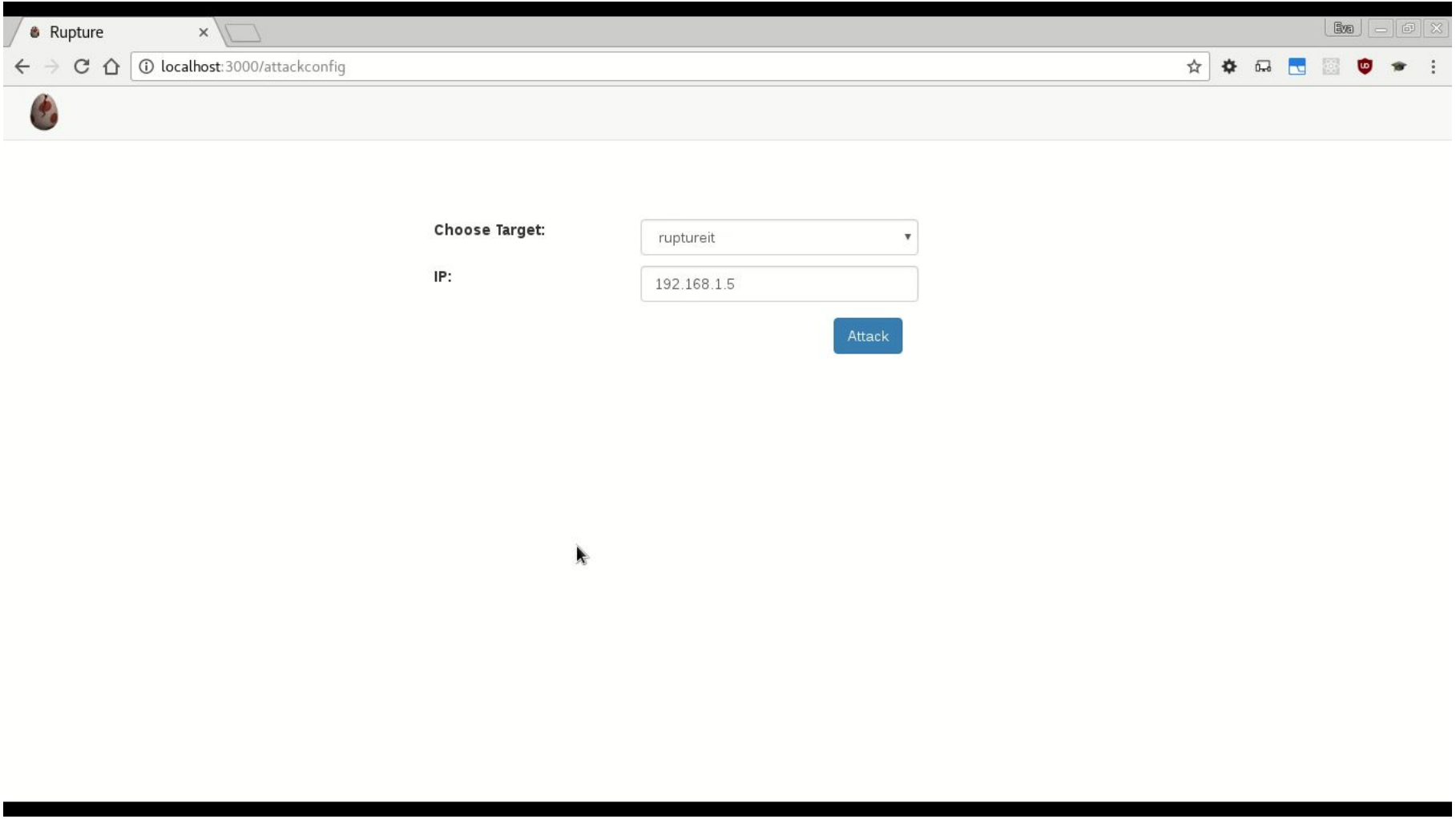
Not started
192.168.1.5

Not started
192.168.1.4

Scan for victims

Add custom victim

RuptureIt


Rupture
localhost:3000/attackconfig
Choose Target:
ruptureit
IP:
192.168.1.5
Attack

Choose Target: Demo

IP: 192.168.1.5

Attack

Rupture

localhost:3000

Network Overview

Completed

Running & Paused

running
192.168.1.5
Demo

0:0:2
more details

Scan for victims

Add custom victim

Not started

RuptureIt

Rupture

localhost:3000

running
192.168.1.5
Demo

0:0:2
more details

Add custom victim

Scan for victims

Not started

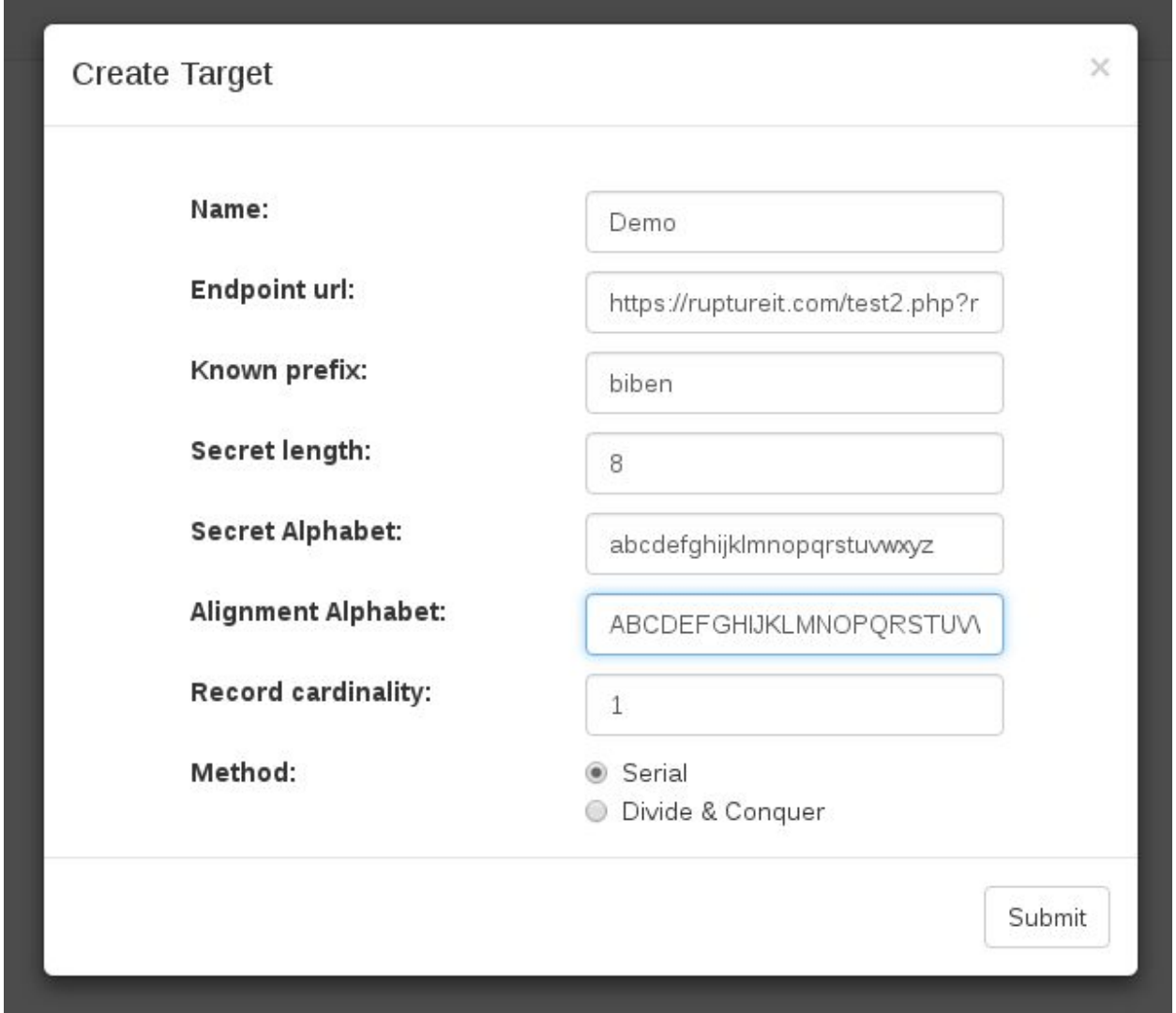
Not started
192.168.1.1

Not started
192.168.1.2

Not started
192.168.1.4

RuptureIt


Choose Target:
ruptureit
IP:
192.168.1.2
Attack


Create Target
Name:
Demo
Endpoint url:
https://ruptureit.com/test2.php?r
Known prefix:
biben
Secret length:
8
Secret Alphabet:
abcdefghijklmnopqrstuvwxyz
Alignment Alphabet:
ABCDEFGHIJKLMNOPQRSTUV\
Record cardinality:
1
Method:
Serial
Divide & Conquer
Submit

Demo

192.168.1.5

Decrypted secret: biben

Round	Batch	Alignment Alphabet	Possible Knownprefix	Confidence
1	1	NQIPLUJDCKBMYEAHTSZGOFWVRX	bibend	0.546875

Delete Pause

Demo

192.168.1.5

Decrypted secret: biben

Round	Batch	Alignment Alphabet	Possible Knownprefix	Confidence
1	1	NQIPLUJDCKBMYEAHTSZGOFWVRX	bibend	0.546875
1	2	TIROYSXHEKJMBADGLZPWUVFCNQ	bibend	0.5

Delete Pause

Demo

192.168.1.5

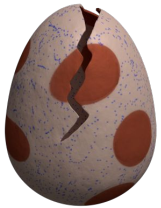
Decrypted secret: biben

Round	Batch	Alignment Alphabet	Possible Knownprefix	Confidence
1	1	NQIPLUJDCKBMYEAHTSZGOFWVRX	bibend	0.546875
1	2	TIROYSXHEKJMBADGLZPWUVFCNQ	bibend	0.5
1	3	QBCRAVWFMHYZTNGOLKDJISUPXE	bibend	0.578125

Delete Pause

https://github.com/dionyziz/rupture

https://ruptureit.com/



Thank you! Questions?

https://github.com/dionyziz/rupture

http://www.kiayias.com

E5F2 7045 437B 168B 39AD 1BFA C876 8019 6DBB 04E0

https://esarafianou.github.io

2FA9 7528 9554 F1EB F5F8 675B E371 5849 8CD0 92EE

https://dionyziz.com

45DC 00AE FDDF 5D5C B988 EC86 2DA4 50F3 AFB0 46C7