Mathy Vanhoef

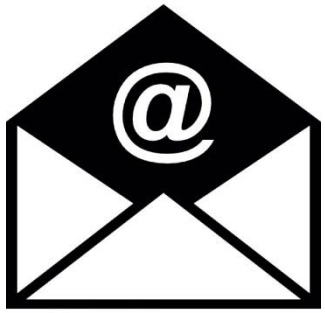
Public PhD Defense

A Security Analysis of the WPA-TKIP and TLS Security Protocols

DistriNet
iMinds
KU LEUVEN

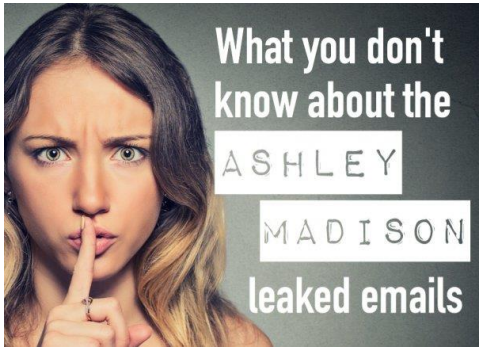
Data handled by computers:

Banking details



Emails

Messaging



Adult websites

Private files

Mobile devices

Goal of dissertation

Is the **transmission** of this data properly protected?

How is data transmitted?

Computer

Wireless router

Server

Study security of network protocols used at:

1. Your wireless network
2. Your internet connection

DistriNet iMinds KU LEUVEN

How is data transmitted?

Computer

Wireless router

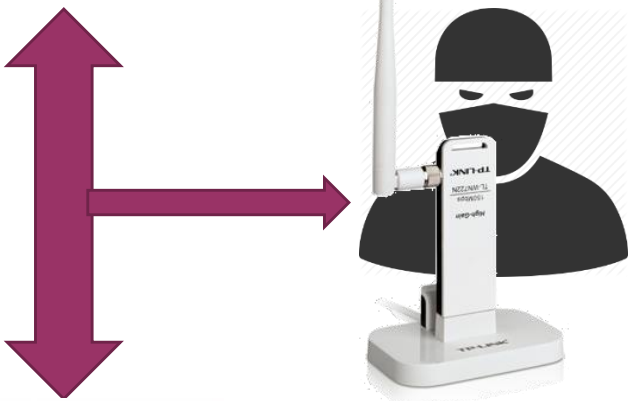
Server

Study security of network protocols used at:

1. **Your wireless network**
2. Your internet connection

Wireless network security

Computer



Wireless router

Easy to intercept transmitted data

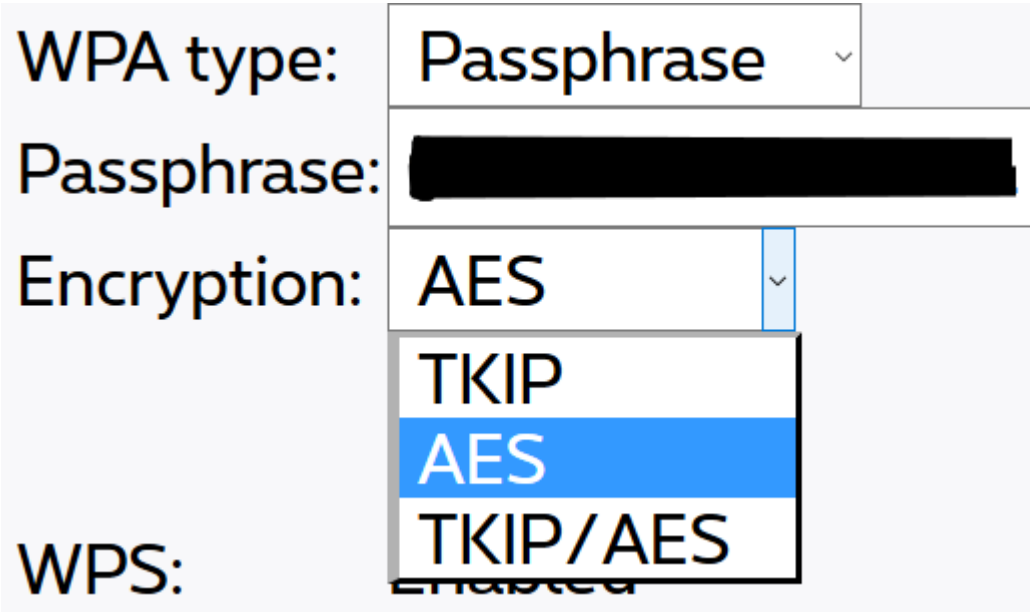
Solution: pick password and use encryption!

Available cipher suites?

WEP WPA-TKIP AES-CCMP

Available cipher suites?

1999	2003	2004
WEP	WPA-TKIP	AES-CCMP
Broken	~~Acceptable~~	Secure



Is WPA-TKIP still used?

Usage in 2013:

66% support TKIP

19% support only TKIP

Need more arguments to kill TKIP!

Is WPA-TKIP still used?

Usage in 2016:

59% support TKIP

3% support only TKIP

Need more arguments to kill TKIP!

Discovered new attacks

1. Efficient Denial of Service
2. Forge arbitrary packets to client
3. Decrypt traffic towards client

In 2016, 59% of networks still are vulnerable!

Impact of attack

unique address for every computer

Website

2.2.2.2

Wireless router

Where is detijd.be?

Computer

Impact of attack

Website
2.2.2.2

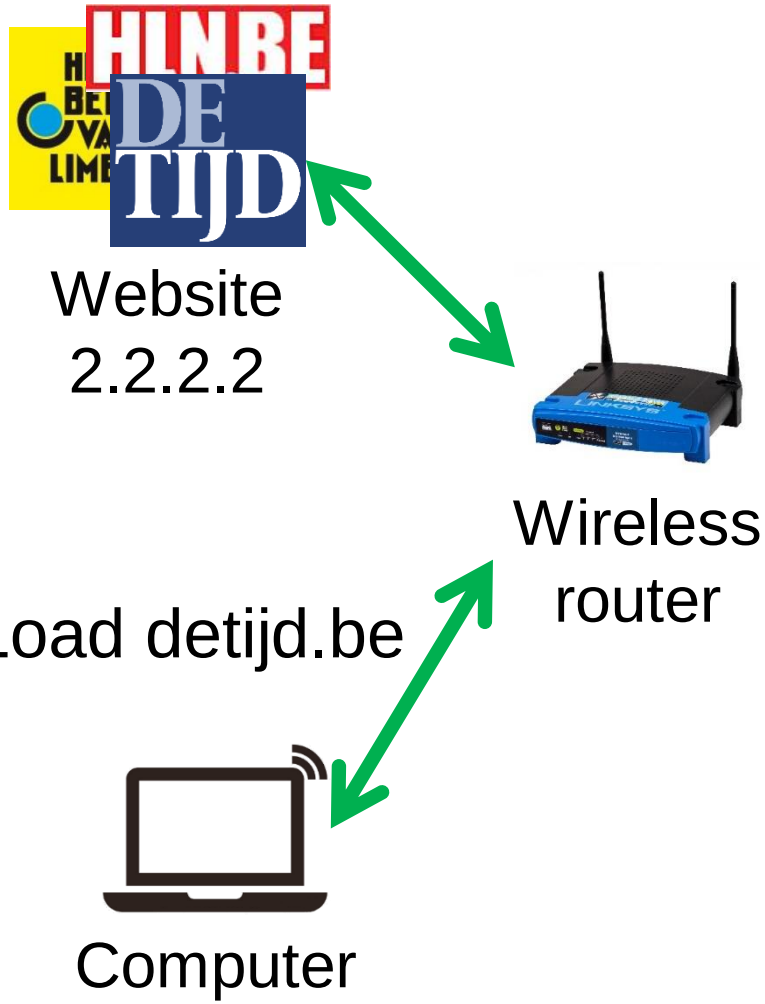
unique address for every computer

Wireless router

detijd.be is at 2.2.2.2

Computer

Impact of attack



Impact of attack

Website
2.2.2.2

Wireless
router

Load detijd.be

Computer

detijd.be is at 4.4.4.4

Attacker
4.4.4.4

Impact of attack

Website
2.2.2.2

Wireless
router

Victim now contacts
attacker to load detijd.be

Load detijd.be

Computer

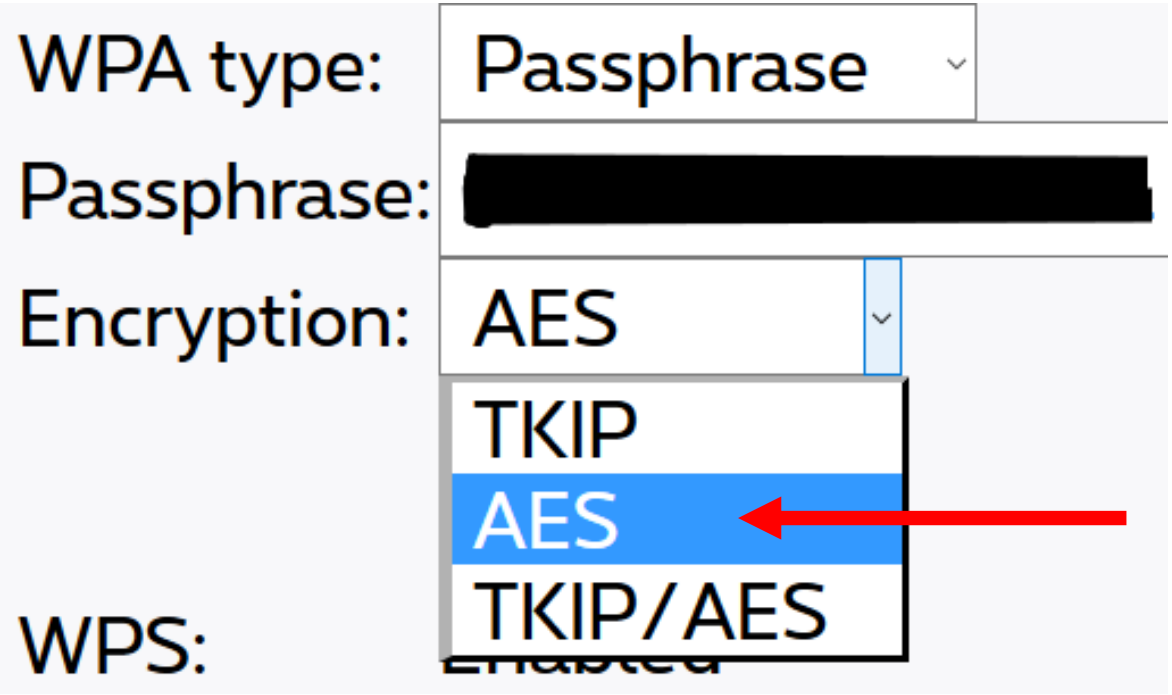
detijd.be is at 4.4.4.4

Attacker
4.4.4.4

DistriNet
iMinds KU LEUVEN

Conclusion

Use only AES-CCMP!



How is data transmitted?

Computer

Wireless router

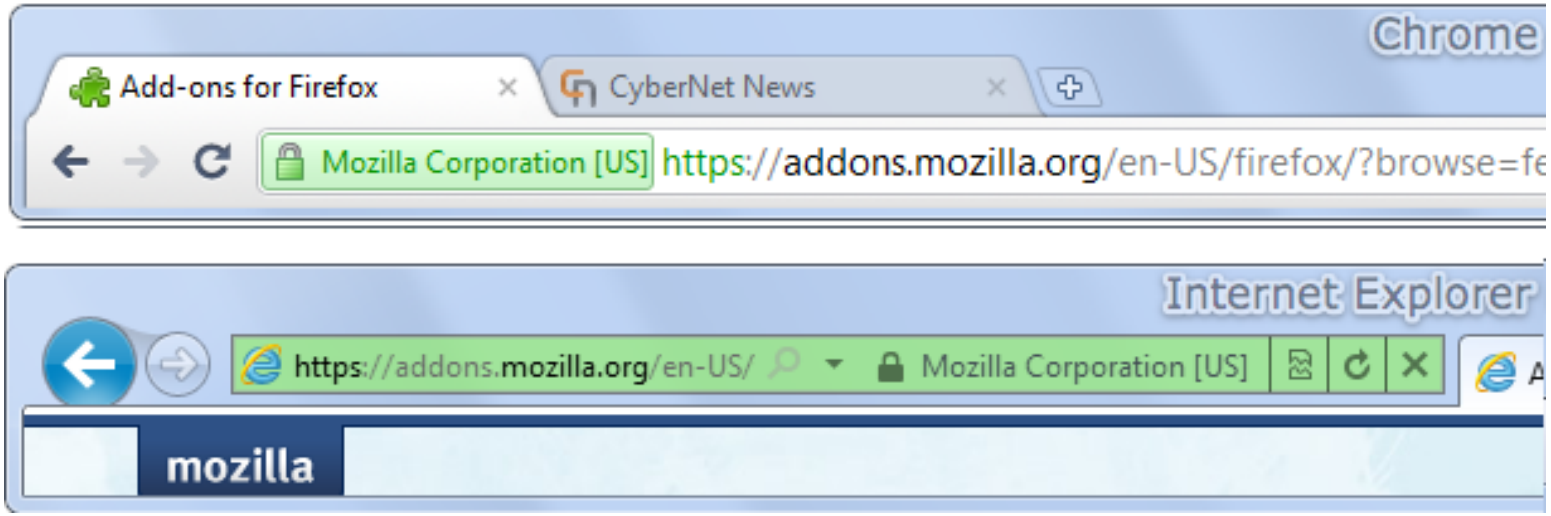
Server

Study security of network protocols used at:

1. Your wireless network
2. **Your internet connection**

Securing internet traffic

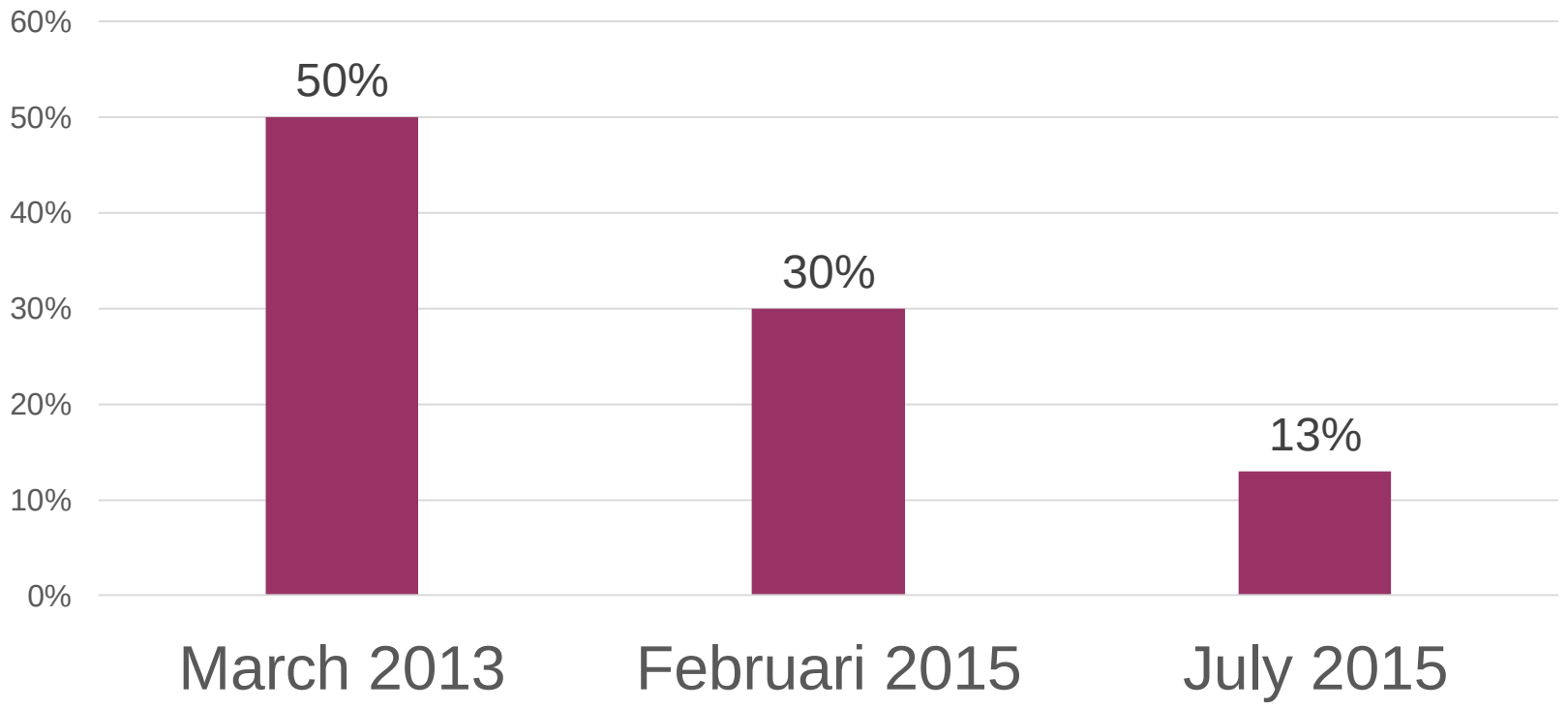
- Websites can be secured using HTTPS



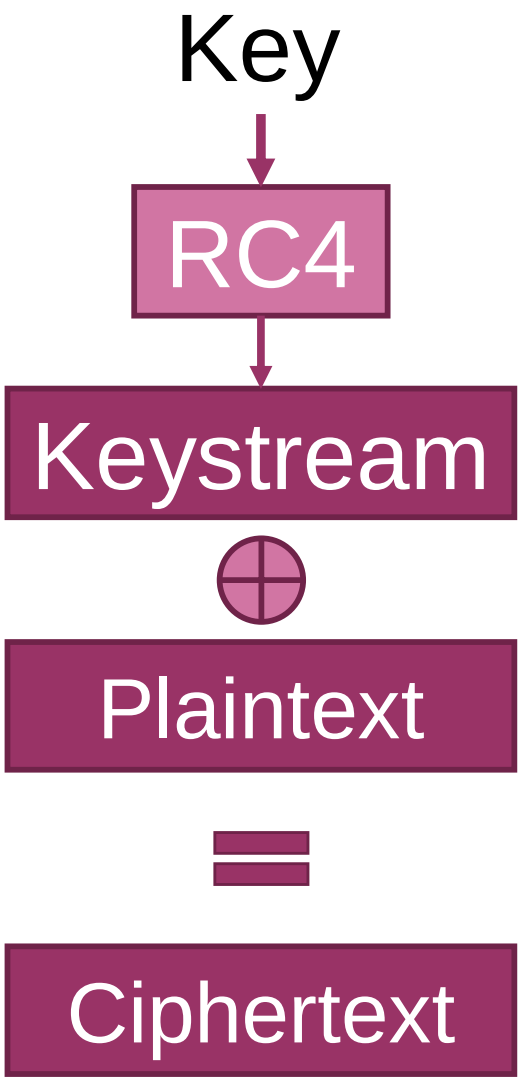
- HTTPS is based on **TLS**
- Internally TLS can use AES, RC4,…
- Which one is widely used? Is it secure?

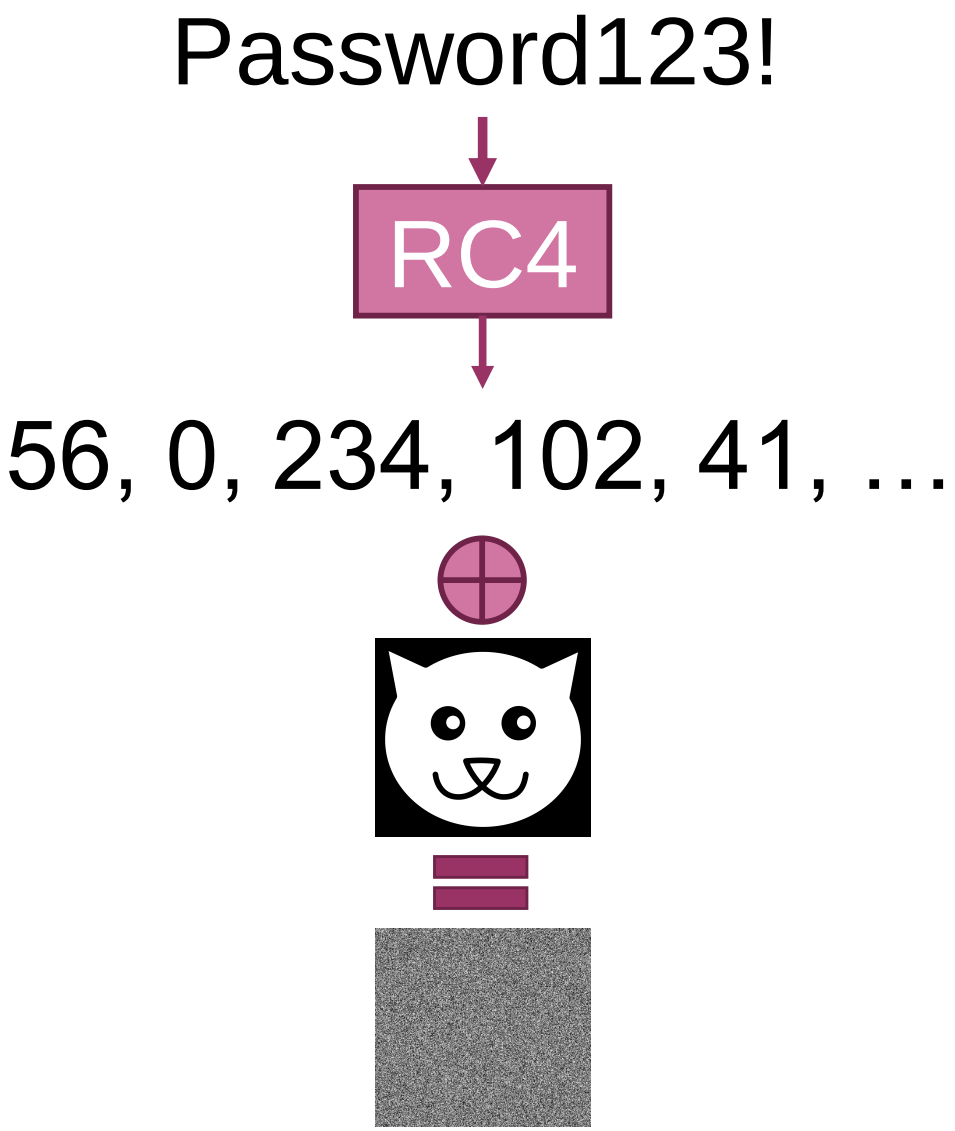
Is RC4 still used?

In 2013 half of all TLS connections used RC4



RC4 encryption





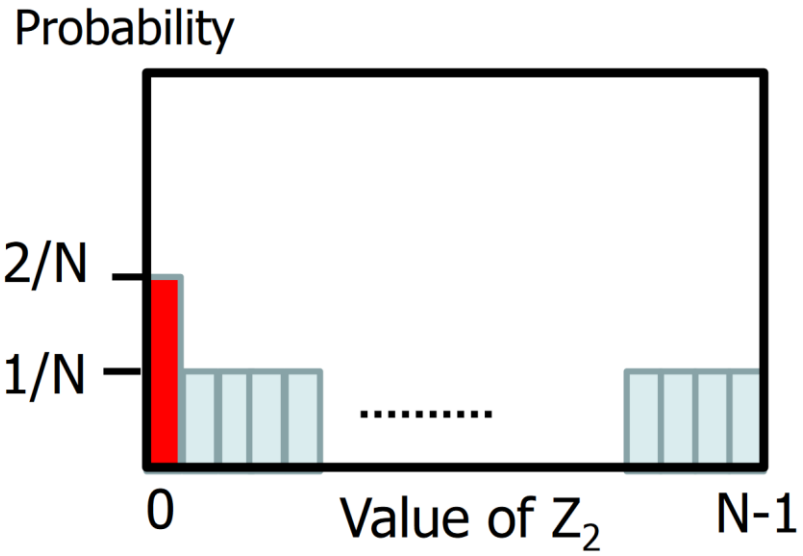
RC4 encryption

- The numbers (keystream) should be random
- Not the case for RC4 due to **biases**!

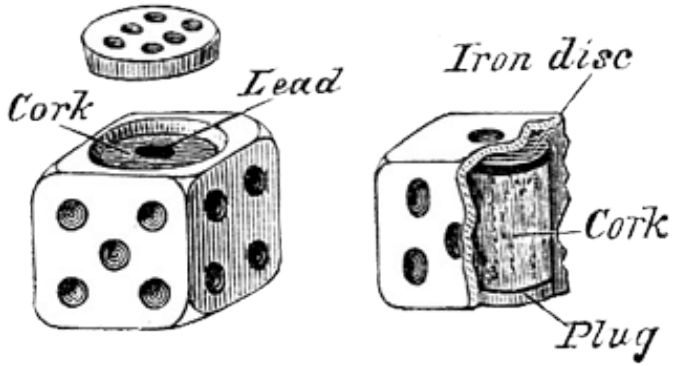
RC4 encryption

Password123! → RC4 → 56, 0, 234, 102, …

- The numbers (keystream) should be random
- Not the case for RC4 due to **biases**!

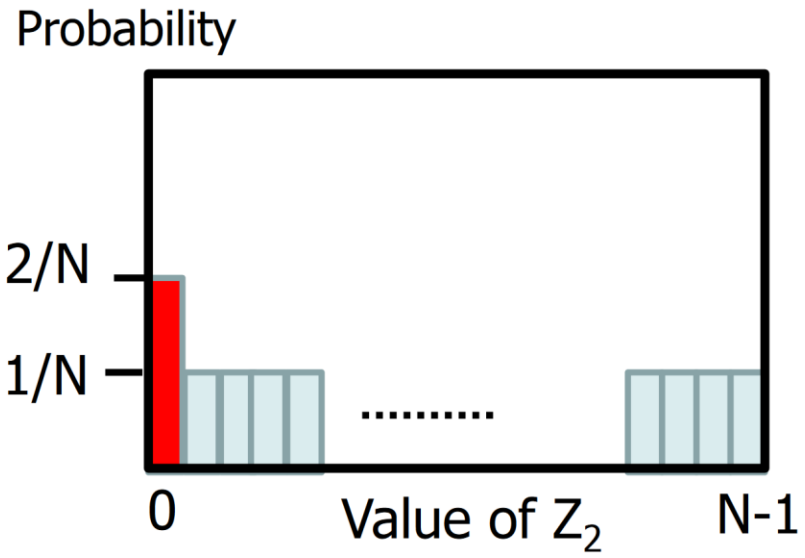


≈

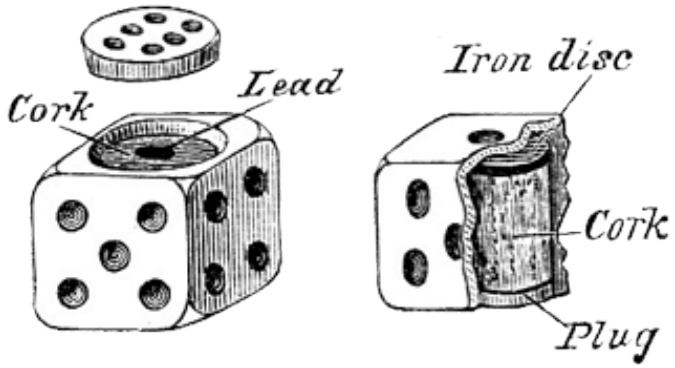


Why is this bad?

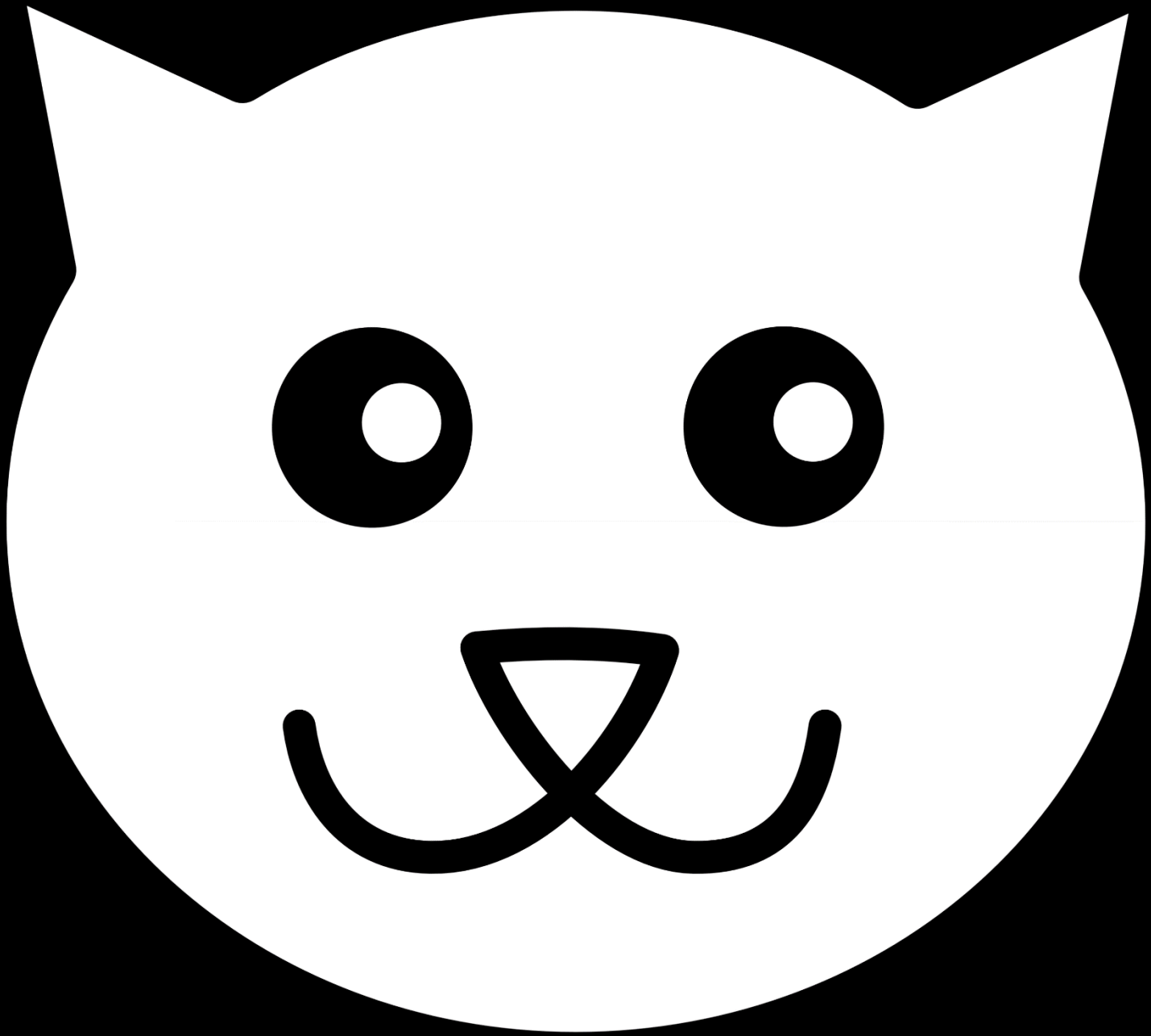
- Imagine only second keystream byte is used



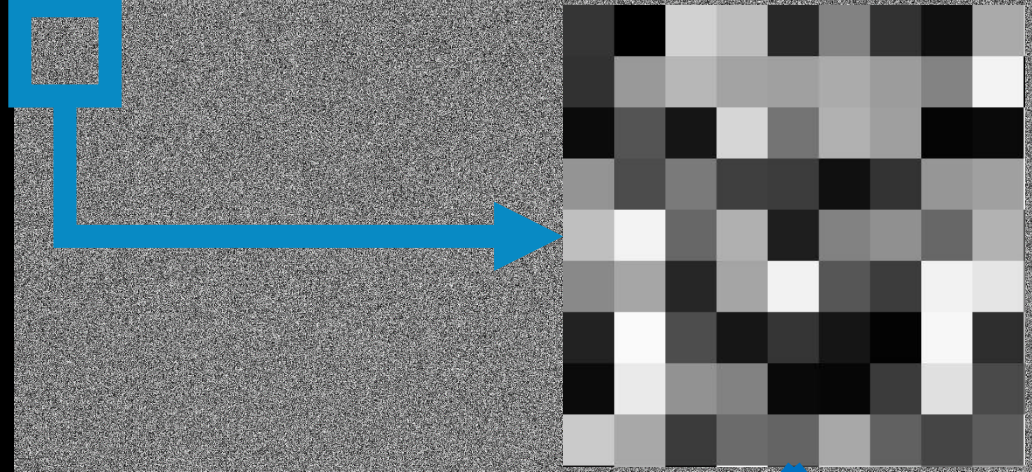
≈



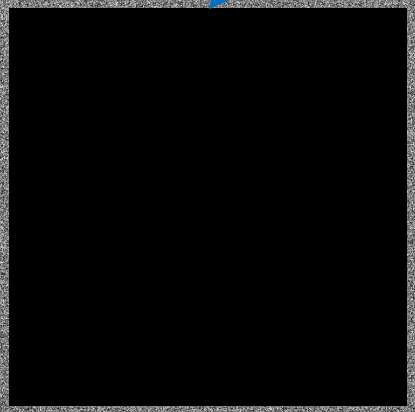
- When is zero is ‘rolled’, no encryption occurs
- Most frequent ciphertextbyte is the real value



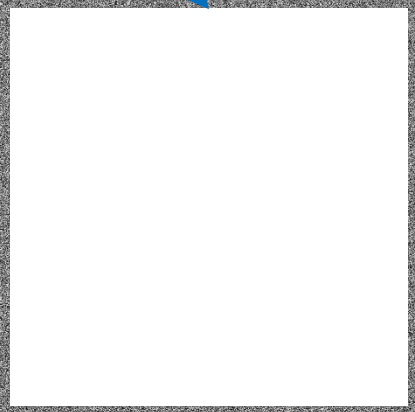
After encryption, image is unrecognizable

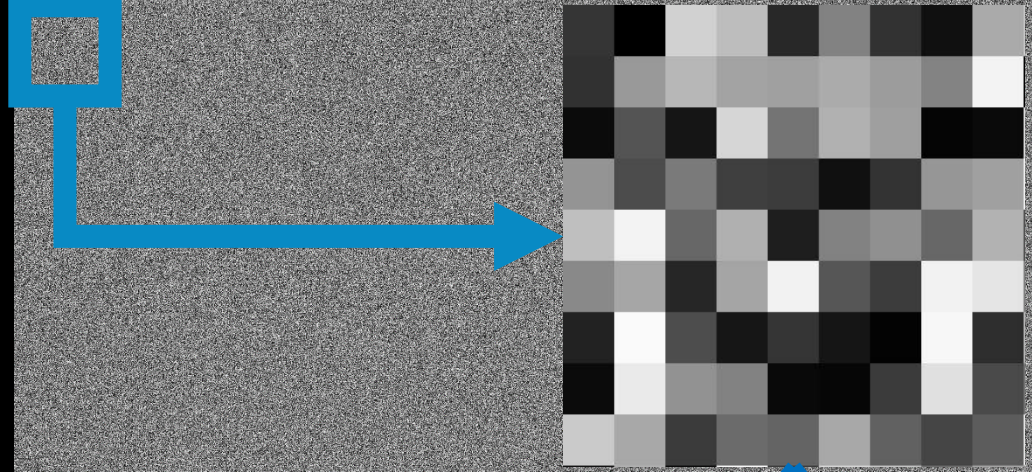


RC4 biases → Most frequent pixel value is the real value

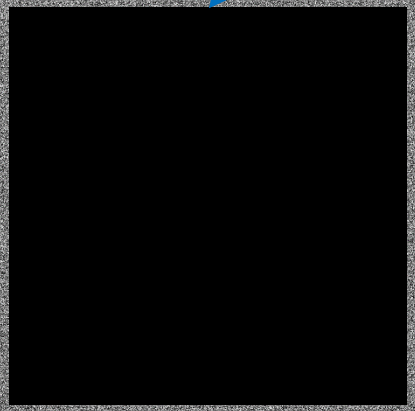


?

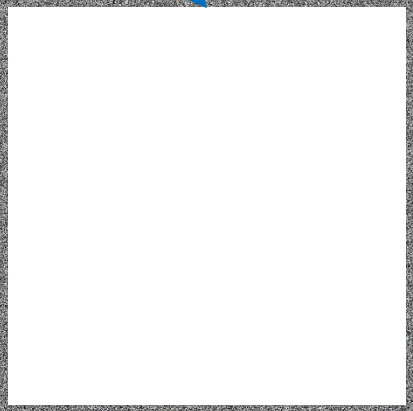


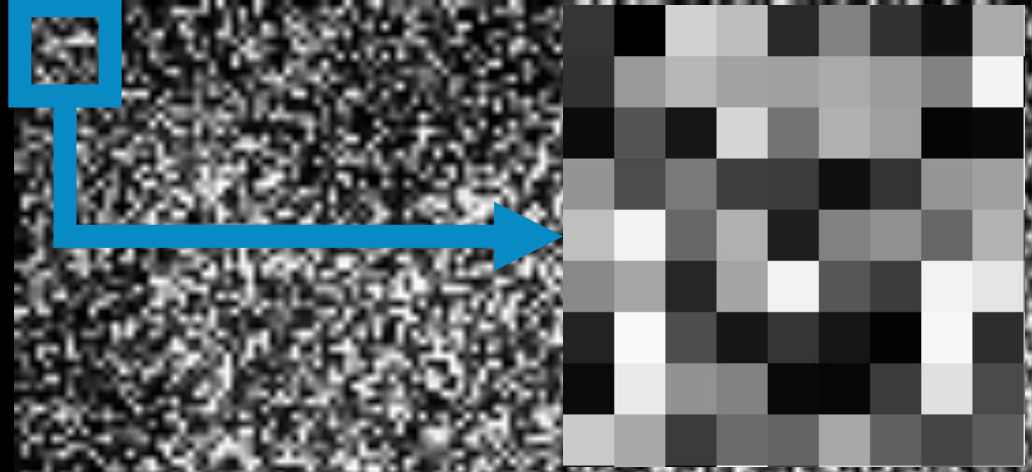


Replace all pixels in block with most frequent value!

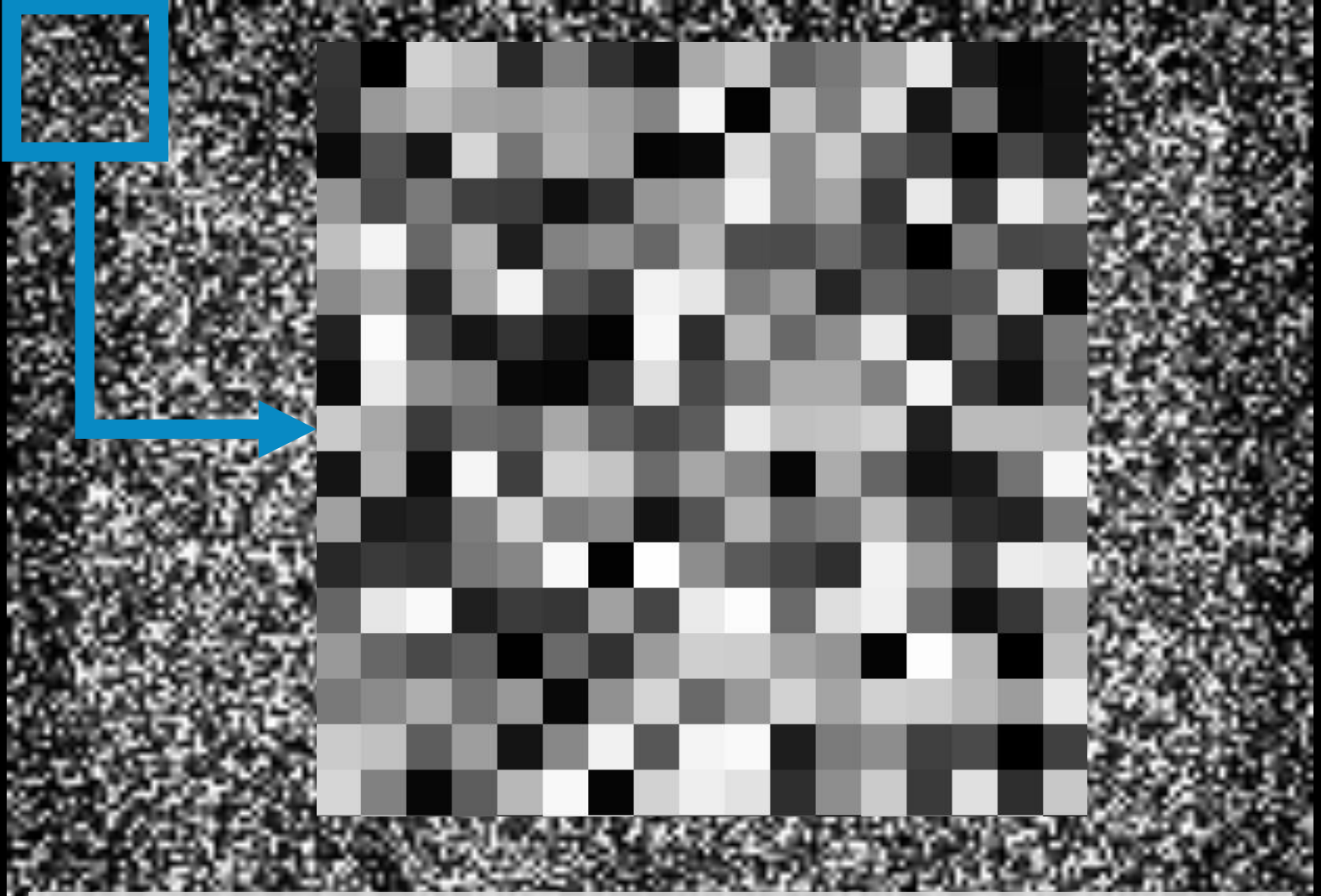


?





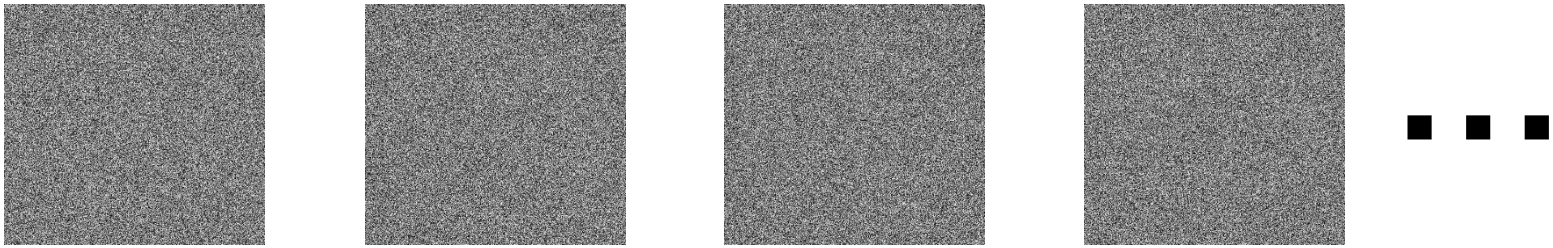
Try to recover rough outline using bigger blocks?



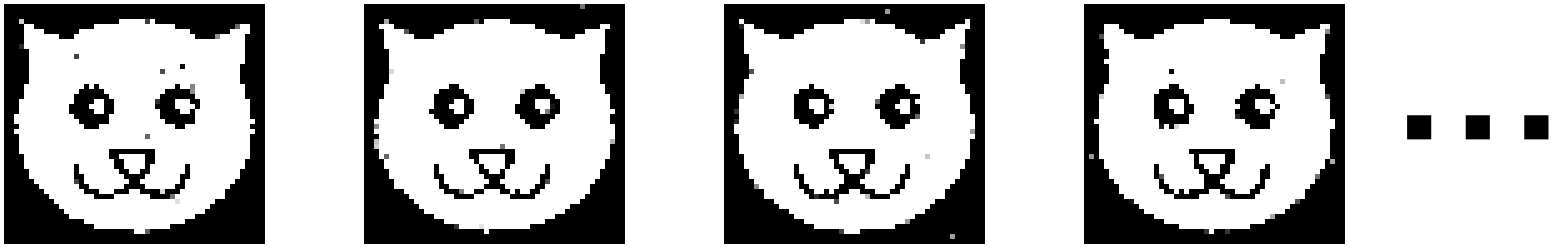
Try to recover rough outline using bigger blocks?

How to recover details?

- Capture multiple encryptions!

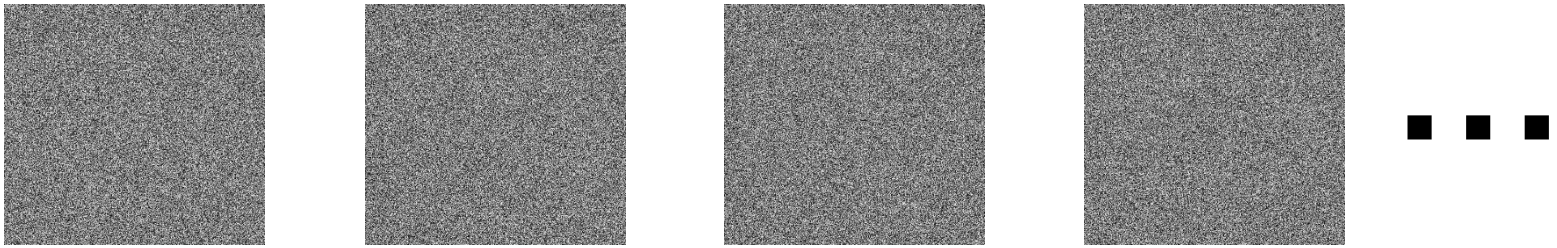


- Combine with biases to recover all info:

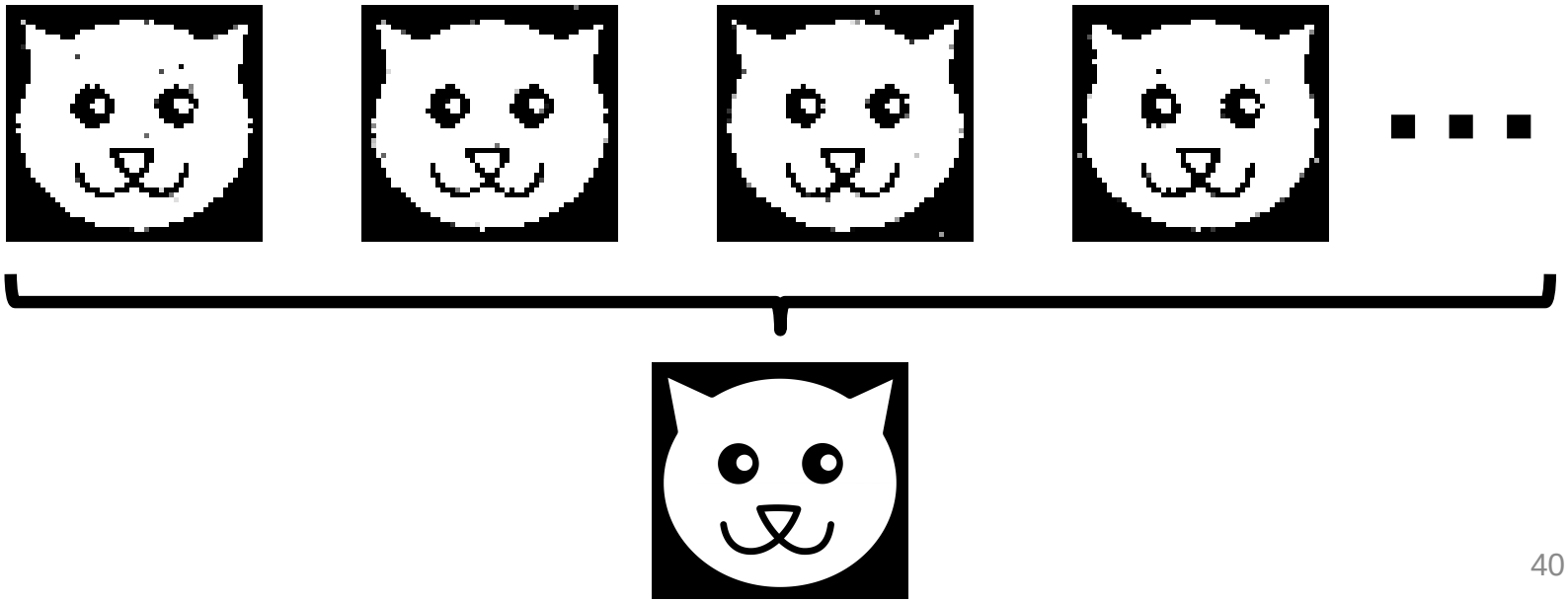


How to recover details?

- Capture multiple encryptions:

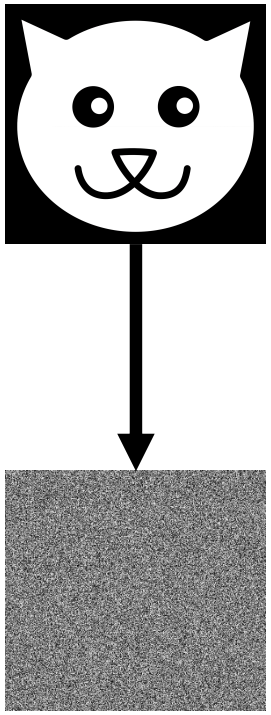


- Combine with biases to recover all info:

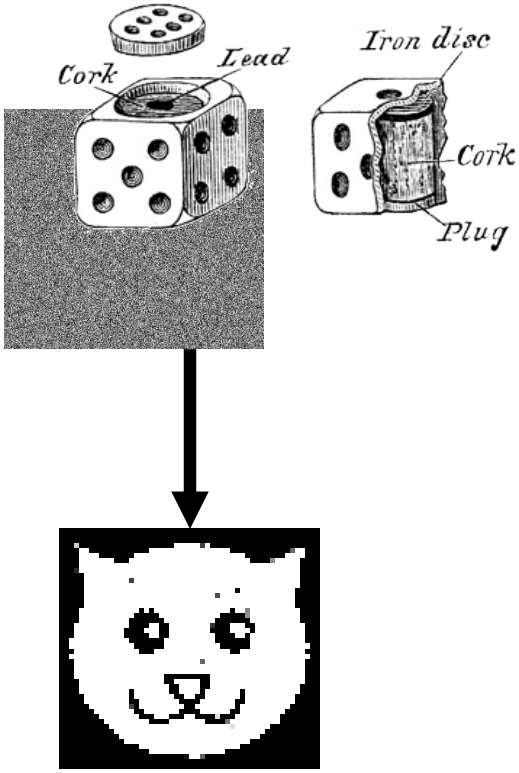


Summary: abusing RC4 biases

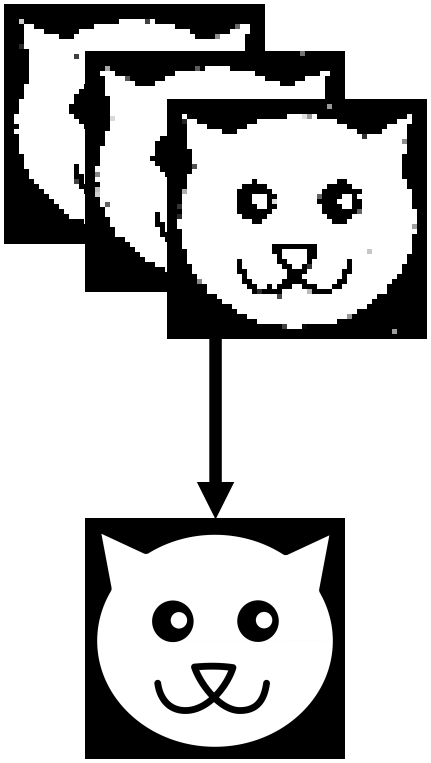
Encryption



Use Biases



Multiple Encryptions



Our contributions

We improved these techniques by:

- Also using other biases
- Generating a list of plaintext candidates
- Rapidly generating multiple encryptions

Using this we decrypt a HTTPS cookie.

Cookies are unique identifiers

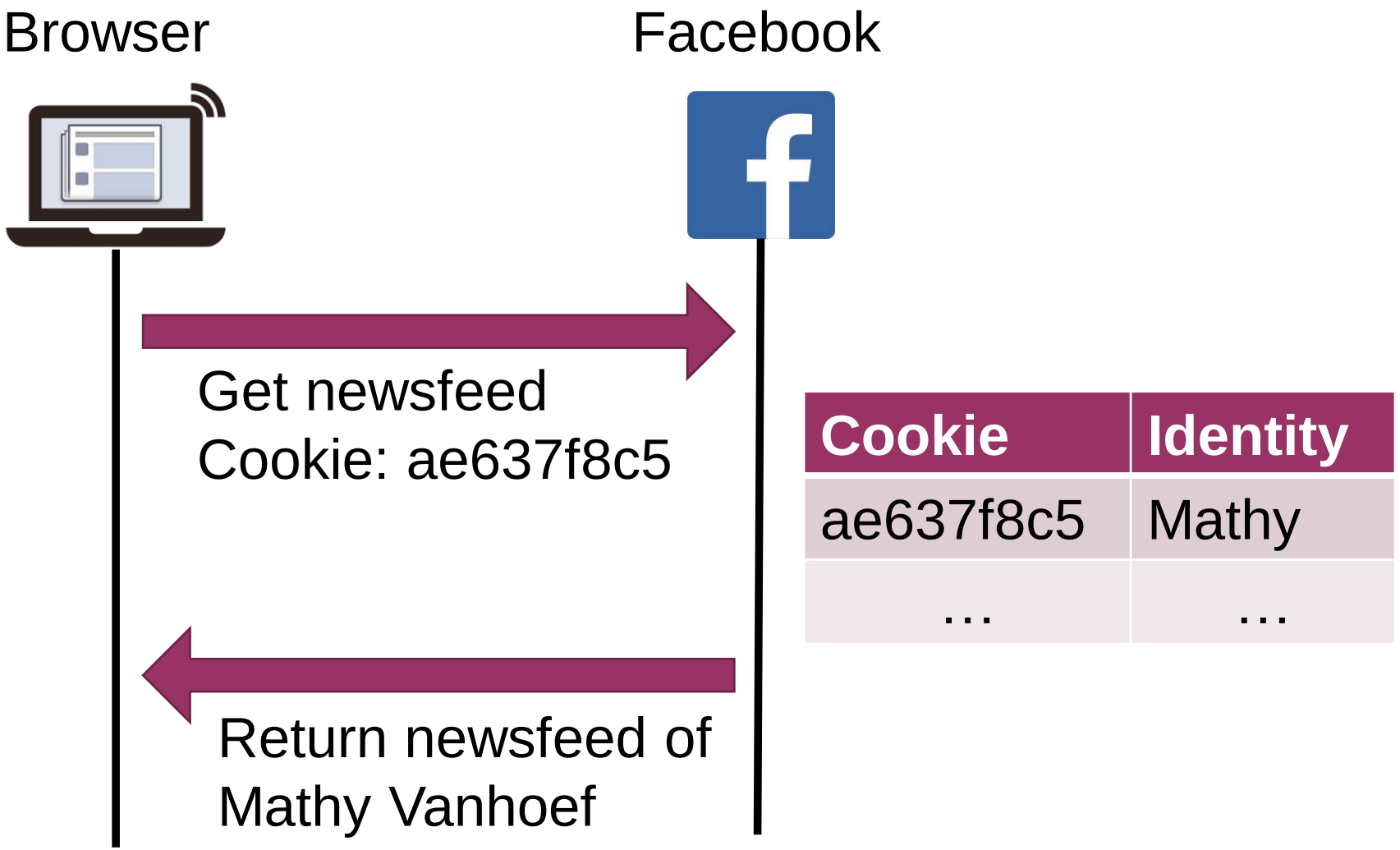
Browser

Facebook

Get newsfeed
Cookie: ae637f8c5

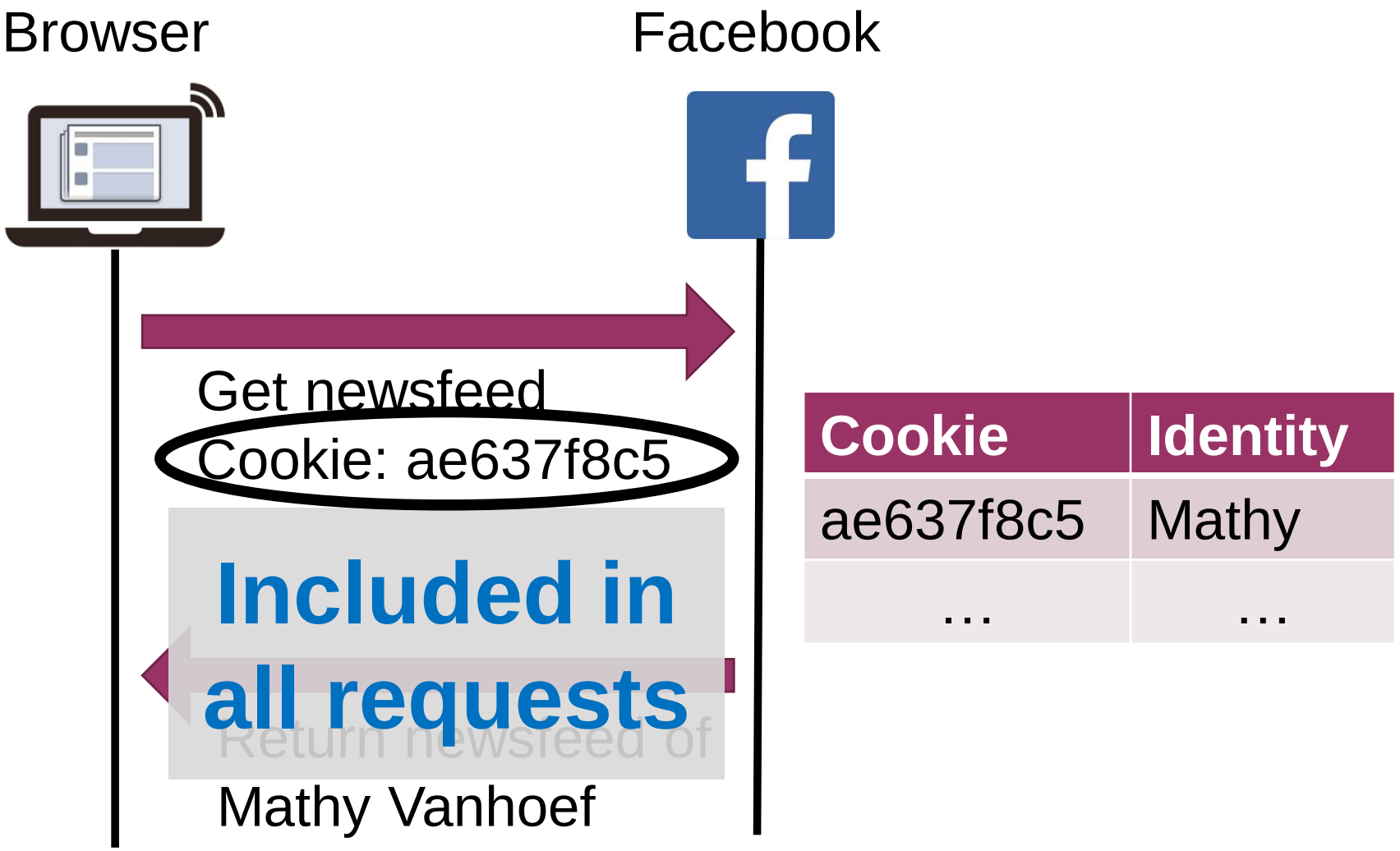
Cookie	Identity
ae637f8c5	Mathy
…	…

Cookies are unique identifiers



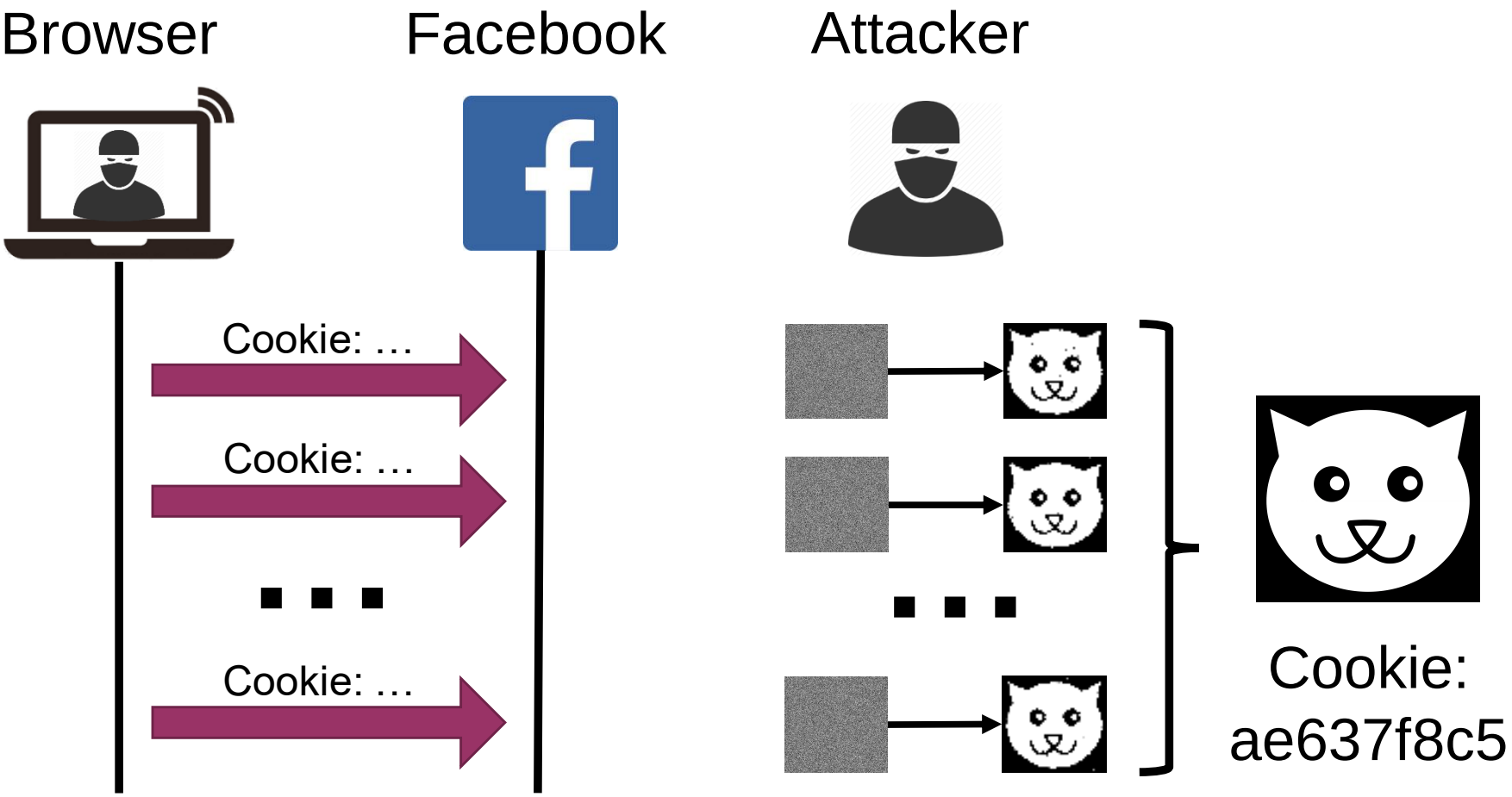
Cookie	Identity
ae637f8c5	Mathy
…	…

Cookies are unique identifiers



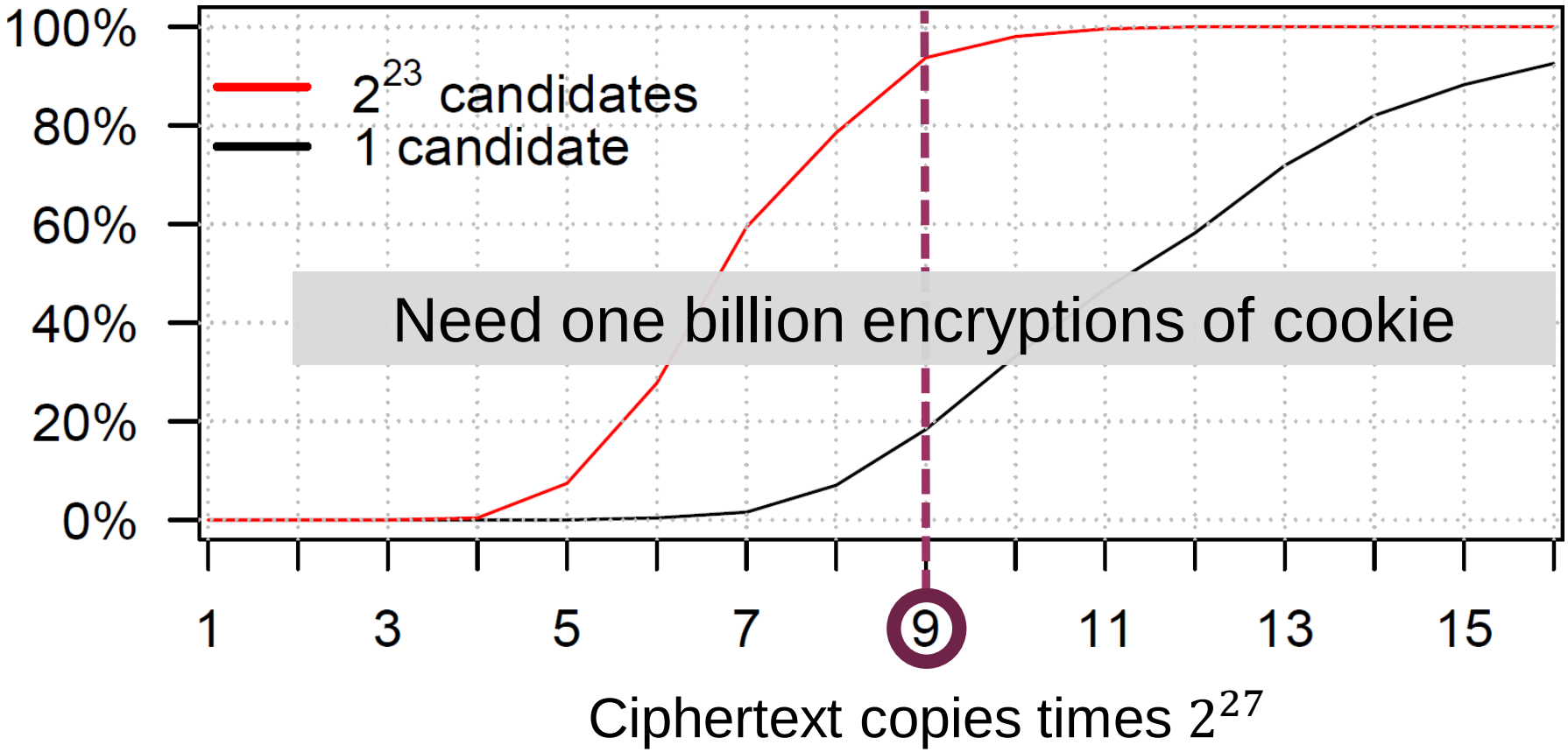
Cookie	Identity
ae637f8c5	Mathy
…	…

Decrypting the cookie

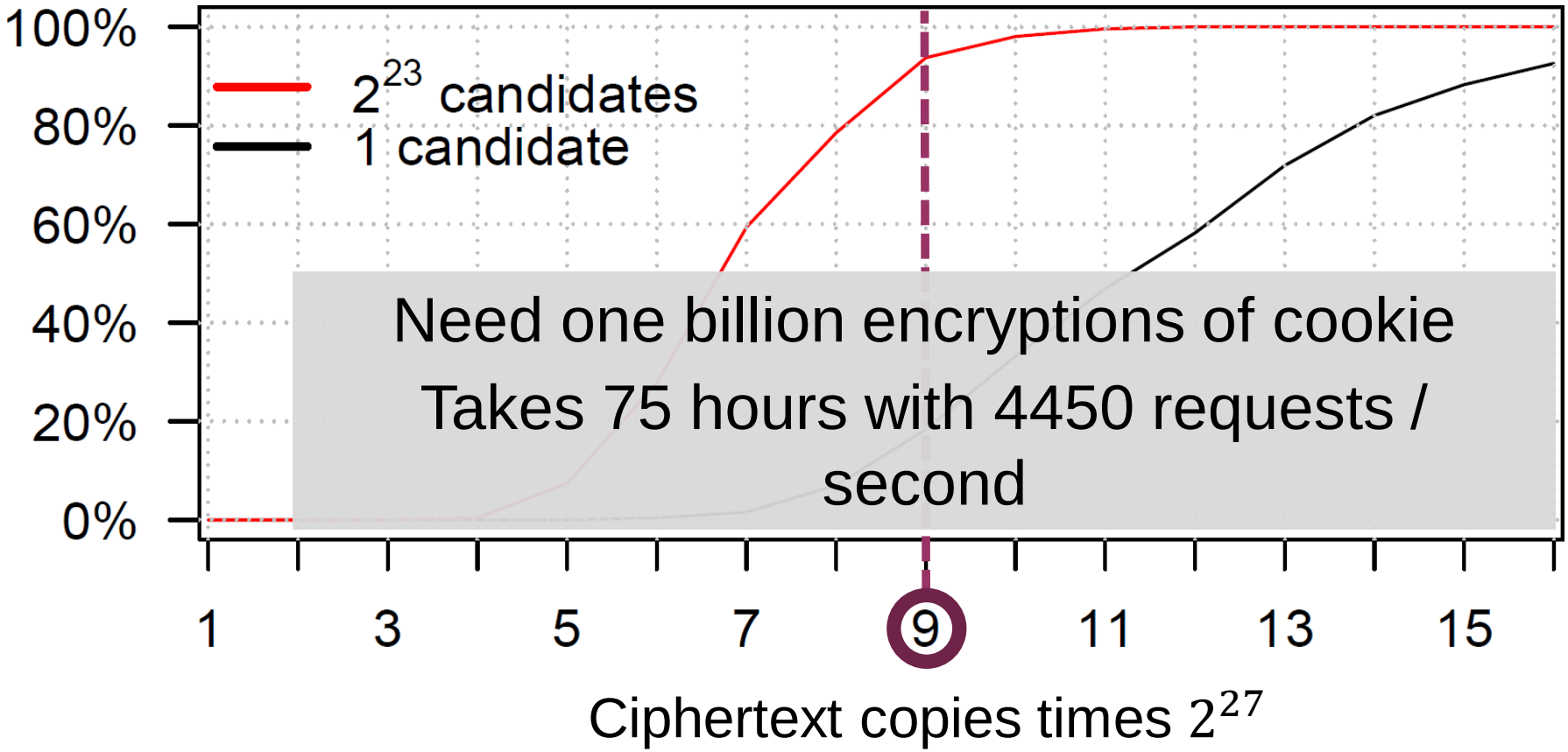


- Generate many requests, use biases to recover the cookie!

Decrypting 16-character cookie



Decrypting 16-character cookie



Practical impact

In response, browsers disabled RC4:

Chrome: dropped support in v48 (20 Jan. 2016)

Firefox: dropped support in v44 (26 Jan. 2016)

IE11: supports RC4

Edge: supports RC4

"will be disabled in forthcoming update"


DEMO!

Questions?