HOW TO BACKDOOR DIFFIE-HELLMAN

David Wong

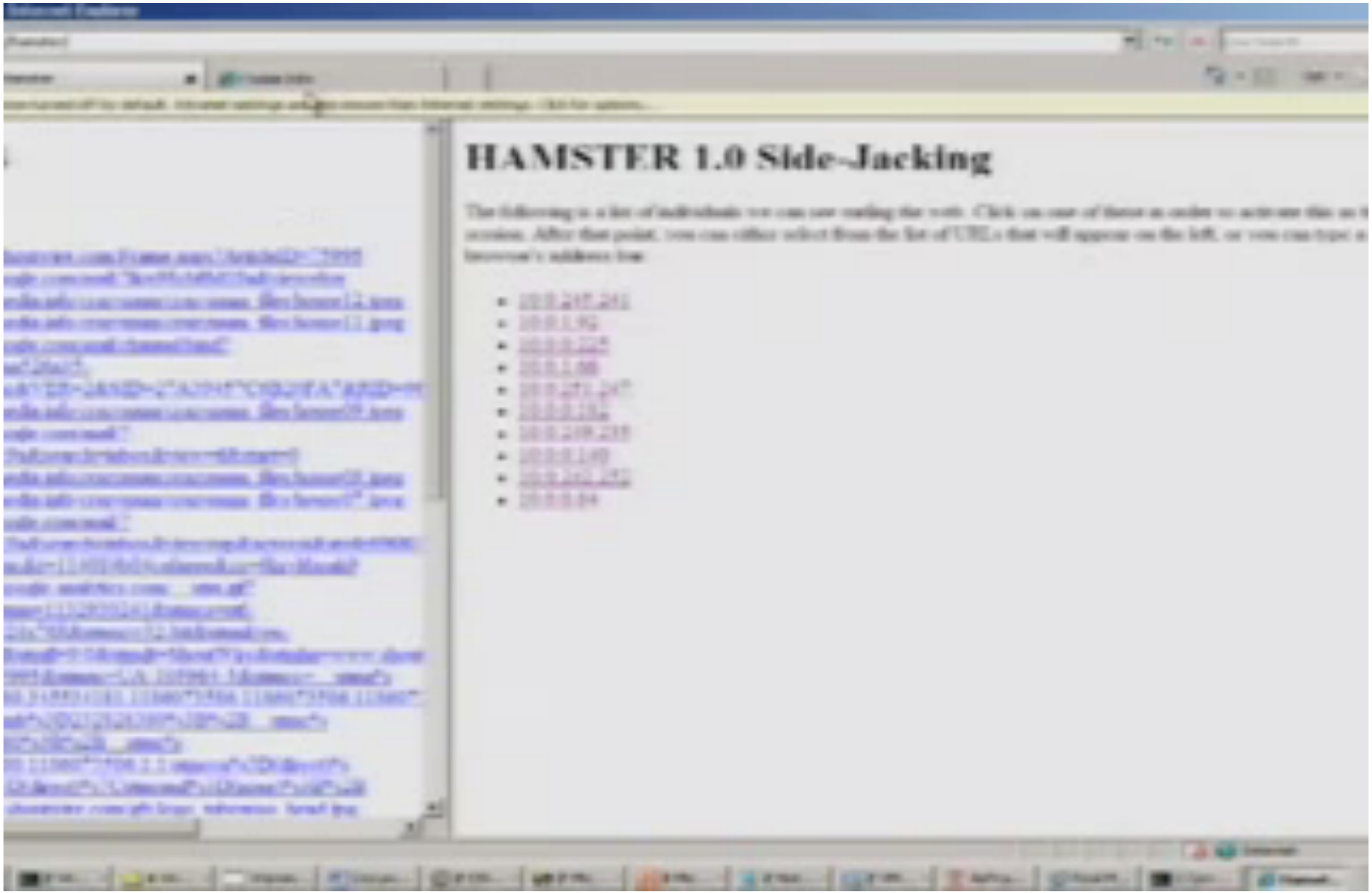
NCC Group

TLS

- *pre-2007*: **Absence** of TLS

TLS

- *pre-2007*: **Absence** of TLS
- *2007*: TLS only for login forms (Graham sniffs gmail **cookies** live at Blackhat)

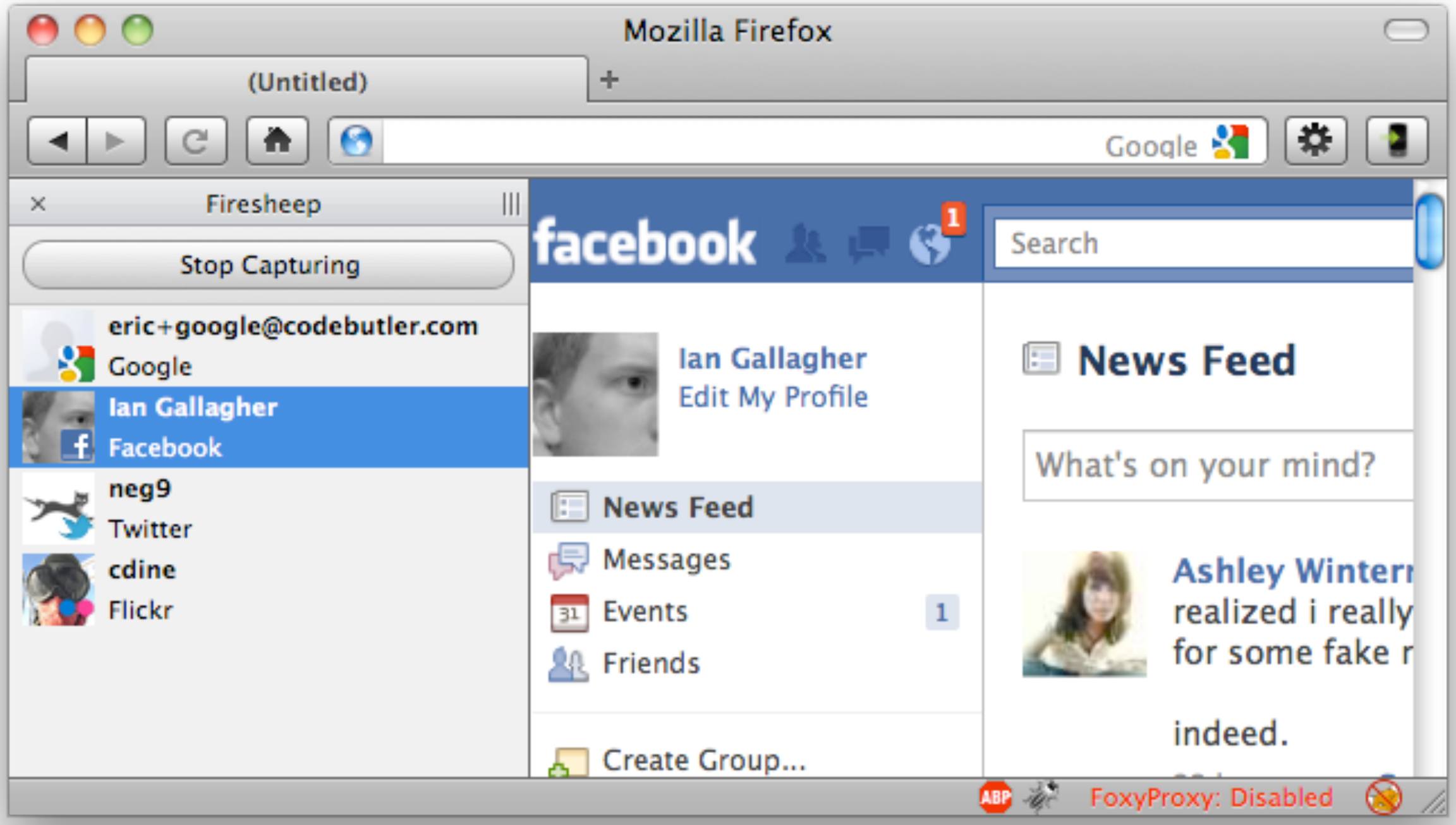

HAMSTER 1.0 Side-Jacking

TLS

- *pre-2007*: **Absence** of TLS
- *2007*: TLS only for login forms (Graham sniffs gmail **cookies** live at Blackhat)
- *2009*: Moxie releases **SSLstrip** at Blackhat

TLS

- *pre-2007*: **Absence** of TLS
- *2007*: TLS only for login forms (Graham sniffs gmail **cookies** live at Blackhat)
- *2009*: Moxie releases **SSLstrip** at Blackhat
- *2010*: **HSTS** introduced in Firefox / Firesheep


Mozilla Firefox
(Untitled)
Google
Firesheep
Stop Capturing
eric+google@codebutler.com
Google
Ian Gallagher
Facebook
neg9
Twitter
cdine
Flickr
facebook
1
Search
Ian Gallagher
Edit My Profile
News Feed
Messages
Events
1
Friends
Create Group...
News Feed
What's on your mind?
Ashley Winter
realized i really
for some fake r
indeed.
ABP
FoxyProxy: Disabled

TLS

- *pre-2007*: **Absence** of TLS
- *2007*: TLS only for login forms (Graham sniffs gmail **cookies** live at Blackhat)
- *2009*: Moxie releases **SSLstrip** at Blackhat
- *2010*: **HSTS** introduced in Firefox / Firesheep
- *2013*: Facebook is **full-https** / **Snowden** leaks

TLS

- *pre-2007*: **Absence** of TLS
- *2007*: TLS only for login forms (Graham sniffs gmail **cookies** live at Blackhat)
- *2009*: Moxie releases **SSLstrip** at Blackhat
- *2010*: **HSTS** introduced in Firefox / Firesheep
- *2013*: Facebook is **full-https** / **Snowden** leaks
- 2010/*2014*: **preloaded-HSTS** introduced in Chrome

Mozilla Security Blog

APR
30
2015

Deprecating Non-Secure HTTP

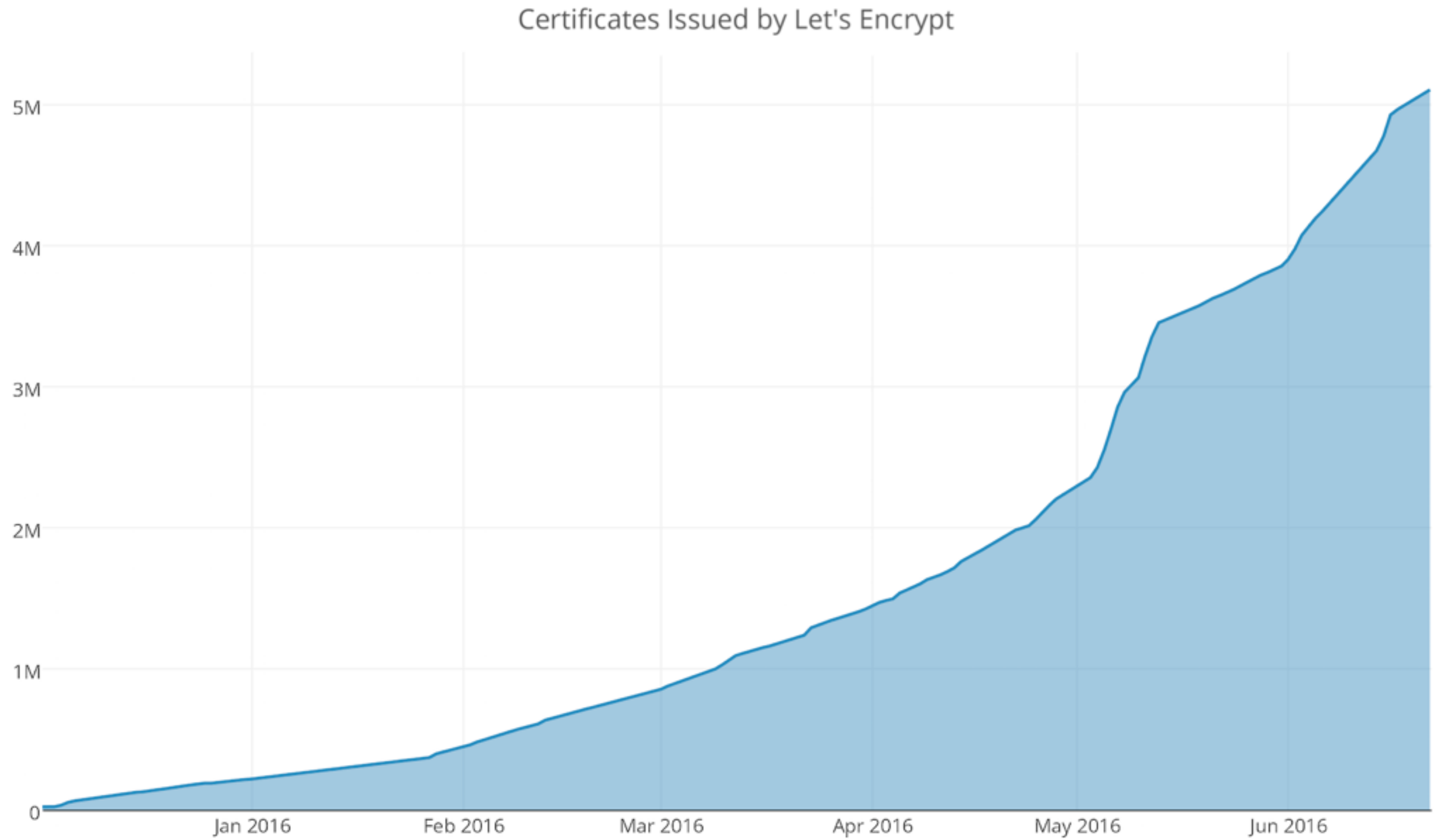
Richard Barnes

288 responses

Today we are announcing our intent to phase out non-secure HTTP.

There's pretty broad agreement that HTTPS is the way forward for the web. In recent months, there have been statements from IETF, IAB (even the other IAB), W3C, and the US Government calling for universal use of encryption by Internet applications, which in the case of the web means HTTPS.

After a robust discussion on our community mailing list, Mozilla is committing to focus new



Let's Encrypt has issued more than 5 million certificates in total since we launched to the general public on December 3, 2015. Approximately 3.8 million of those are active, meaning unexpired and unrevoked. Our active certificates cover more than 7 million unique domains.

Logjam

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice

David Adrian[¶] Karthikeyan Bhargavan[*] Zakir Durumeric[¶] Pierrick Gaudry[†] Matthew Green[§]
J. Alex Halderman[¶] Nadia Heninger[‡] Drew Springall[¶] Emmanuel Thomé[†] Luke Valenta[‡]
Benjamin VanderSloot[¶] Eric Wustrow[¶] Santiago Zanella-Béguelin[‖] Paul Zimmermann[†]

[*] INRIA Paris-Rocquencourt [†] INRIA Nancy-Grand Est, CNRS, and Université de Lorraine
[‖] Microsoft Research [‡] University of Pennsylvania [§] Johns Hopkins [¶] University of Michigan

For additional materials and contact information, visit WeakDH.org.

ABSTRACT

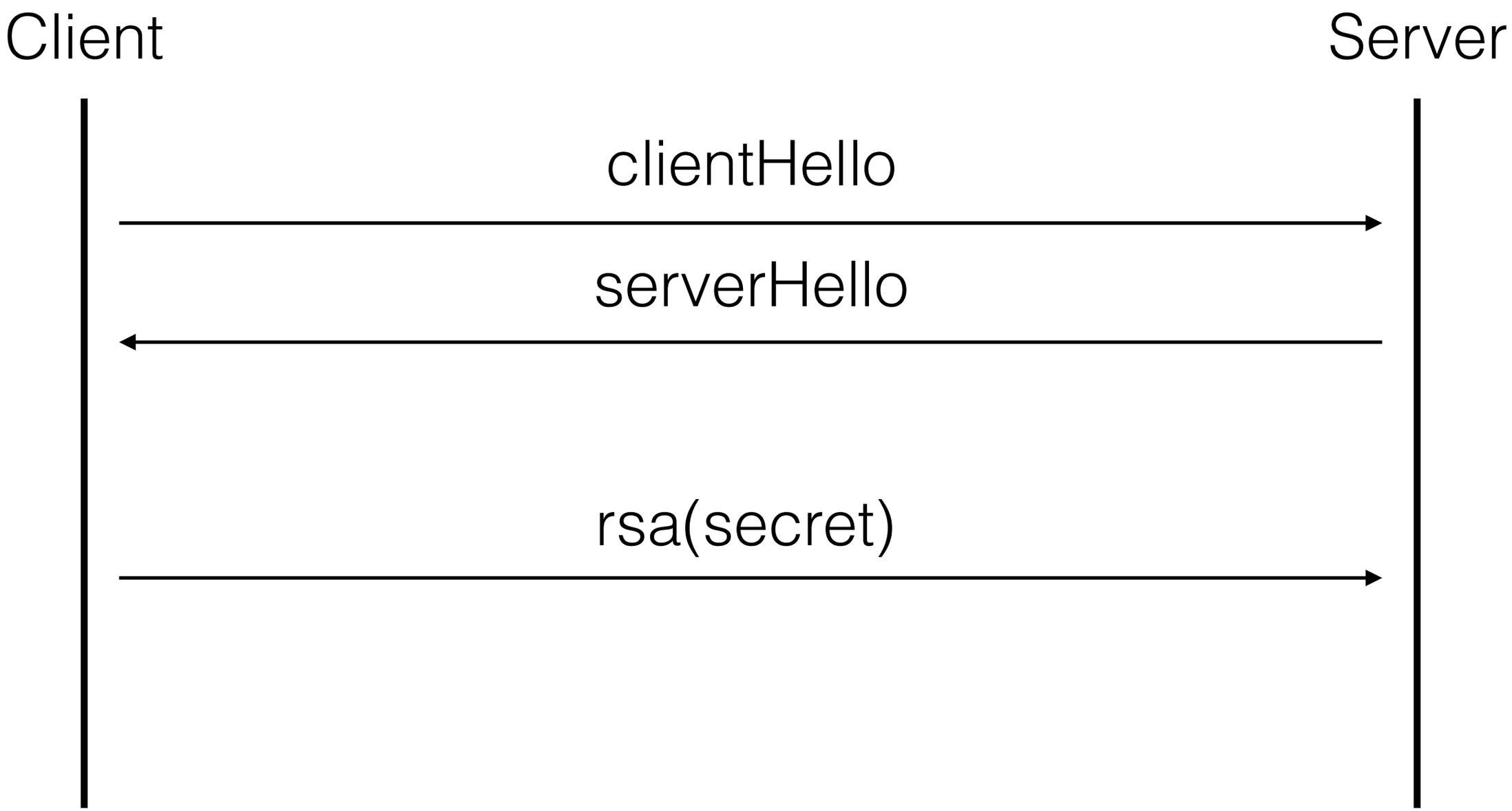
We investigate the security of Diffie-Hellman key exchange as used in popular Internet protocols and find it to be less secure than widely believed. First, we present Logjam, a novel flaw in TLS that lets a man-in-the-middle downgrade connections to "export-grade" Diffie-Hellman. To carry out this attack, we implement the number field sieve discrete log algorithm. After a week-long precomputation for a specified 512-bit group, we can compute arbitrary discrete logs in that group in about a minute. We find that 82% of vulnerable servers use a single 512-bit group, allowing us to compromise connections coded, or widely shared Diffie-Hellman parameters has the effect of dramatically reducing the cost of large-scale attacks, bringing some within range of feasibility today.

The current best technique for attacking Diffie-Hellman relies on compromising one of the private exponents (a, b) by computing the discrete log of the corresponding public value $(g^a \bmod p,\ g^b \bmod p)$. With state-of-the-art number field sieve algorithms, computing a single discrete log is more difficult than factoring an RSA modulus of the same size. However, an adversary who performs a large precomputation for a prime p can then quickly calculate arbitrary discrete logs in that group, amortizing the cost over all targets that share

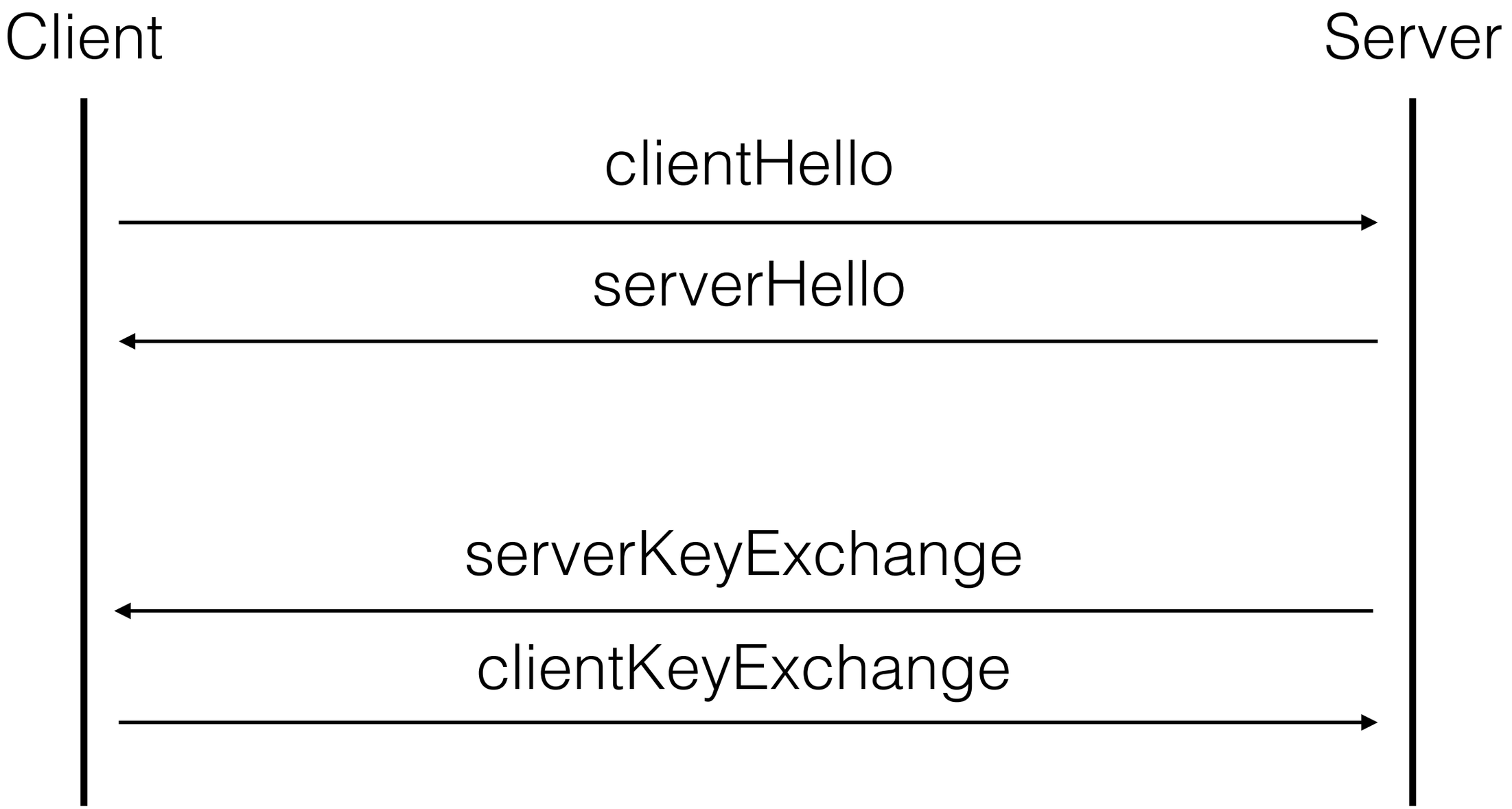
Logjam

- **hardcoded** DHE parameters in Apache

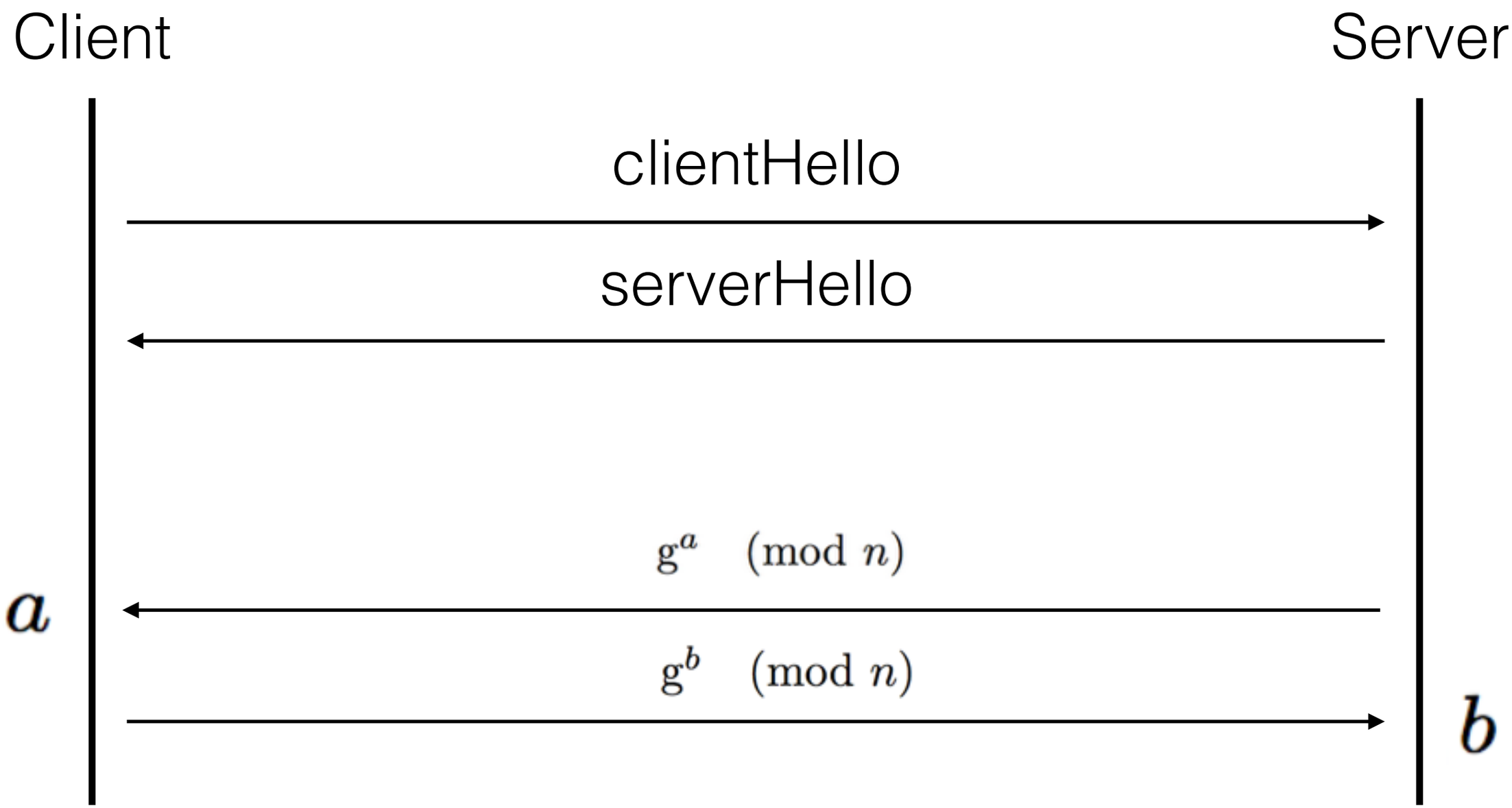
Logjam



Logjam


Client
Server
clientHello
serverHello
serverKeyExchange
clientKeyExchange

Logjam


Client
Server
clientHello
serverHello
$g^a \pmod n$
a
$g^b \pmod n$
b

Logjam

- **hardcoded** DHE parameters in Apache

$$g^a \pmod{n}$$

Logjam

- **hardcoded** DHE parameters in Apache
- NSA believed to be able to compute discrete logarithm in modulo **1024-bit integers**

Logjam

- **hardcoded** DHE parameters in Apache

- NSA believed to be able to compute discrete logarithm in modulo **1024-bit integers**

- **too much work**

U.S. export rules

- **weak** “Export” Cipher Suites

U.S. export rules

- **weak** “Export” Cipher Suites
- **512-bit primes** for Diffie-Hellman

U.S. export rules

- **weak** “Export” Cipher Suites
- **512-bit primes** for Diffie-Hellman
- **40-bit keys** for DES

Mail - Inbox - IBM Lotus Notes

File Edit View Create Actions Tools Window Help

Open | Home | Christine Costner - Mail

Search All Mail

Christine Costner

domino

- Inbox (7)
- Drafts
- Sent
- Follow Up
- All Documents
- Junk
- Trash
- Chat History
- Views
- Folders
- Archive

Follow Up

Remove Flag

When | Who

New | Unified Messaging | Actions... | Call Manager | Reply | Reply to All | Show

- New Fax
- New Text Message
- XPhone UM Settings

Search | Indexed

Search for | Search | Search tips | More

Sender	Subject	Date	Size
Kevin Kramer	Purchase Order 115116114	06/02/2010 09:14	31K
UMServer	Voicemail from Pete Wursch +491762226700	06/02/2010 06:01	51K
UMServer	Fax from Christine Costner +4989840798131	05/02/2010 17:23	33K
UMServer	Fax to +4989840194 Sent successfully	05/02/2010 16:32	117K
UMServer	Voicemail from Kevin Kramer +4989840798	05/02/2010 15:37	130K
UMServer	Fax from Peter Walker +49898407981	05/02/2010 15:23	133K
UMServer	Fax from Pete Wursch +498984079	05/02/2010 14:14	333K
Kevin Kramer	Re: Marketing Meeting Feb	05/02/2010 12:14	3K
UMServer	SMS to +790393997	05/02/2010 10:52	2K

Online

LOTUS NOTES

- 64-bit crypto allowed…

LOTUS NOTES

- 64-bit crypto allowed…
- …if **24 bits of the key are encrypted to the NSA**

LOTUS NOTES

- 64-bit crypto allowed…
- …if **24 bits of the key are encrypted to the NSA**
- NSA's RSA public key

O=MiniTruth CN=Big Brother

Kleptography

- A kleptographic attack is an attack which uses **asymmetric cryptography** to implement a cryptographic **backdoor**.

Kleptography

- A kleptographic attack is an attack which uses **asymmetric cryptography** to implement a cryptographic **backdoor**.

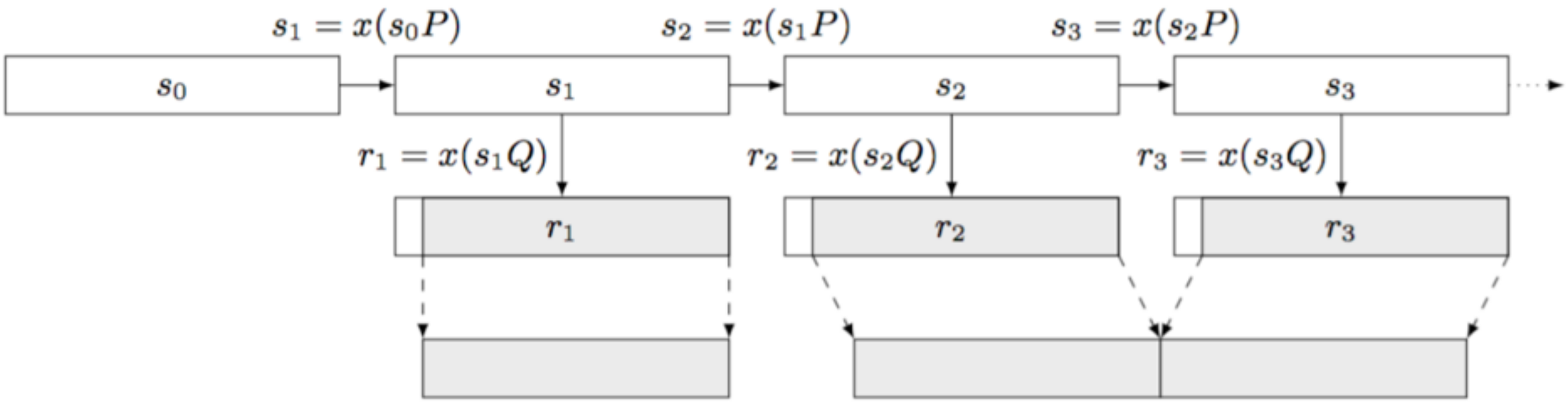
- A secure kleptographic attack is undetectable **as long as the cryptosystem is a black-box**.

Kleptography

- A kleptographic attack is an attack which uses **asymmetric cryptography** to implement a cryptographic **backdoor**.
- A secure kleptographic attack is undetectable **as long as the cryptosystem is a black-box**.
- what about **white-box**? **Reverse Engineering**?

- ~~Weak crypto~~
- ~~Kleptography~~

Dual EC


$s_1 = x(s_0P)$
$s_2 = x(s_1P)$
$s_3 = x(s_2P)$
s_0
s_1
s_2
s_3
$r_1 = x(s_1Q)$
$r_2 = x(s_2Q)$
$r_3 = x(s_3Q)$
r_1
r_2
r_3

NIST Special Publication 800-90A

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Elaine Barker and John Kelsey

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

2007

On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng

Dan Shumow
Niels Ferguson
Microsoft

CRYPTO 2007

NSA's BULLRUN

TOP SECRET//SI//REL TO USA, FVEY

CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry


NSA
BSAFE TOOLKIT®

2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)

▼ [JSA10713] Show KB Properties

PRODUCT AFFECTED:

Please see below for details.

PROBLEM:

During an internal code review, two security issues were identified.

Administrative Access (CVE-2015-7755) allows unauthorized remote administrative access to the device. Exploitation of this vulnerability can lead to complete compromise of the affected device.

This issue only affects ScreenOS 6.3.0r17 through 6.3.0r20. **No other Juniper products or versions of ScreenOS are affected by this issue.**

Upon exploitation of this vulnerability, the log file would contain an entry that '**system**' had logged on followed by password authentication for a username.

Example:

Normal login by user **username1**:

```
2015-12-17 09:00:00 system warn 00515 Admin user username1 has logged on via SSH from …..
2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin
user 'username1' at host …
```

Compromised login by user **username2**:

```
2015-12-17 09:00:00 system warn 00515 Admin user system has logged on via SSH from …..
2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin
user 'username2' at host …
```

Note that a skilled attacker would likely remove these entries from the local log file, thus effectively eliminating any reliable signature that the device had been compromised.

This issue has been assigned CVE-2015-7755

patched

juniper — david@little-david — ~/Tests/juniper

```
[λ ~/Tests/juniper/ strings ssg5ssg20.6.3.0r19b.0.bin | grep -C5 -i "6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296\|]
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7\|c6858e06b70404e9cd9e3ecb662395b4429c
648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66"
CLOSING
TIME_WAIT
FFFFFFFF0000000100000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFF0000000100000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFC
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
2c55e5e45edf713dc43475effe8813a60326a64d9ba3d2e39cb639b0f3b0ad10
EC PRNG KAT failure
CLOSE
LISTEN
```

vulnerable

juniper — david@little-david — ~/Tests/juniper

```
[λ ~/Tests/juniper/ strings ssg5ssg20.6.3.0r19.0.bin | grep -C5 -i "6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296\|a]
a87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7\|c6858e06b70404e9cd9e3ecb662395b4429c6
48139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66"
CLOSING
TIME_WAIT
FFFFFFFF0000000100000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFF0000000100000000000000000000000FFFFFFFFFFFFFFFFFFFFFFFC
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
9585320EEAF81044F20D55030A035B11BECE81C785E6C933E4A8A131F6578107
EC PRNG KAT failure
CLOSE
LISTEN
```

Dual EC is **obvious**.

- ~~Weak crypto~~
- ~~Kleptography~~
- ~~New Backdoored Algorithms~~

Date: Mon, 1 Feb 2016 16:32:55 +0100
From: Gerhard Rieger <gerhard@...t-unreach.org>
To: oss-security@...ts.openwall.com
Subject: Socat security advisory 7 - Created new 2048bit DH modulus

Socat security advisory 7 - Created new 2048bit DH modulus

Overview
  In the OpenSSL address implementation the hard coded 1024 bit DH p
  parameter was not prime. The effective cryptographic strength of a key
  exchange using these parameters was weaker than the one one could get by
  using a prime p. Moreover, since there is no indication of how these
  parameters were chosen, the existence of a trapdoor that makes possible
  for an eavesdropper to recover the shared secret from a key exchange that
  uses them cannot be ruled out.
  A new prime modulus p parameter has been generated by Socat developer
  using OpenSSL dhparam command.
  In addition the new parameter is 2048 bit long.

Vulnerability Ids:
  Socat security issue 7
  MSVR-1499

Severity: Unknown

Affected versions

Date: Mon, 1 Feb 2016 16:32:55 +0100
From: Gerhard Rieger <gerhard@...t-unreach.org>
To: oss-security@...ts.openwall.com
Subject: Socat security advisory 7 - Created new 2048bit DH modulus

Socat security advisory 7 - Created new 2048bit DH modulus

Overview
  In the OpenSSL address implementation the hard coded 1024 bit DH p
  parameter was not prime. The effective cryptographic strength of a key
  exchange using these parameters was weaker than the one one could get by
  using a prime p. Moreover, since there is no indication of how these
  parameters were chosen, the existence of a trapdoor that makes possible
  for an eavesdropper to recover the shared secret from a key exchange that
  uses them cannot be ruled out.
  A new prime modulus p parameter has been generated by Socat developer
  using OpenSSL dhparam command.
  In addition the new parameter is 2048 bit long.

Vulnerability Ids:
  Socat security issue 7
  MSVR-1499

Severity: Unknown

Affected versions

DHE backdoor?

DHE backdoor?

- Everyone **trust** DHE already

DHE backdoor?

- Everyone **trust** DHE already
- *Logjam*: **hardcoded** DHE everywhere

DHE backdoor?

- Everyone **trust** DHE already
- *Logjam*: **hardcoded** DHE everywhere
- Everyone is **upgrading to 2048-bit parameters**

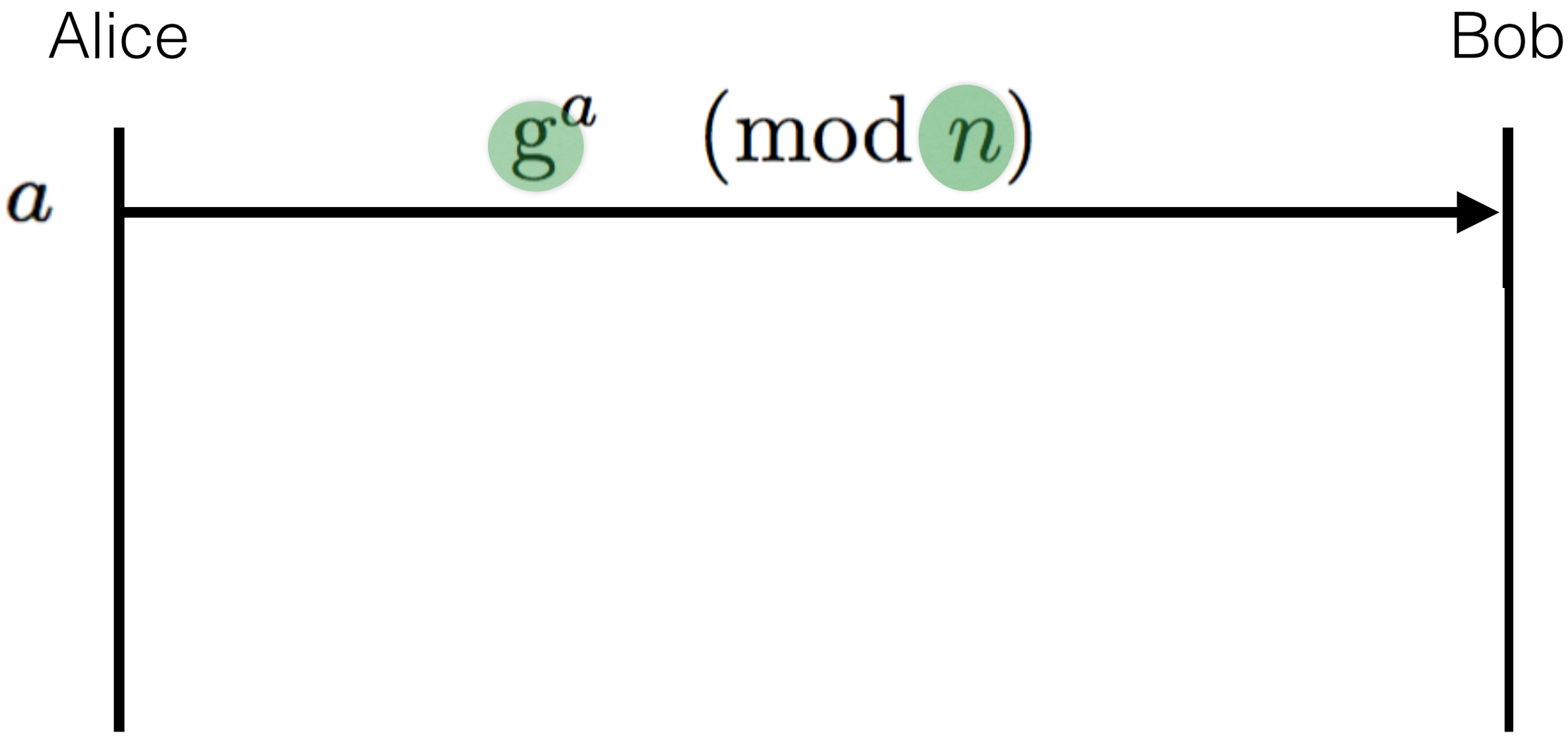
Diffie-Hellman

Alice

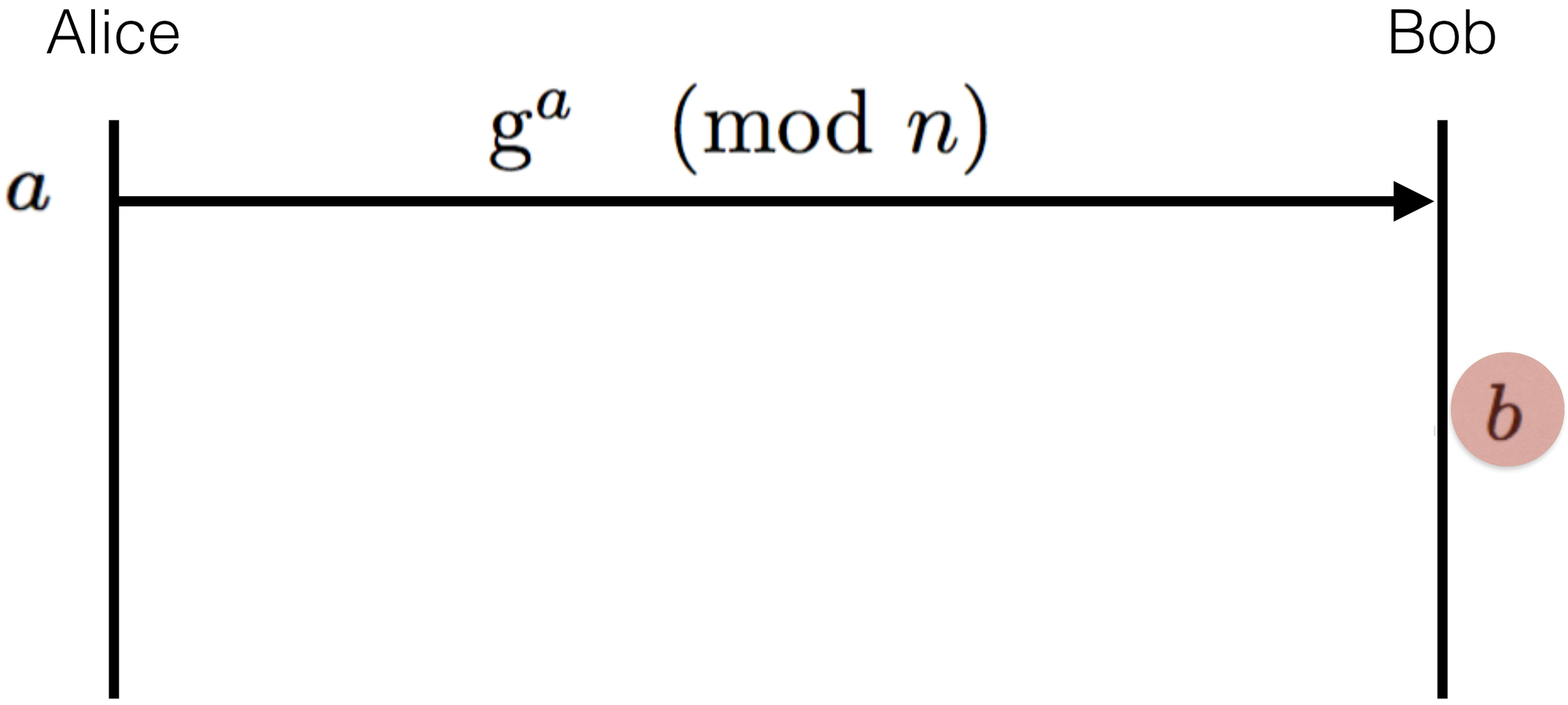
Bob

a

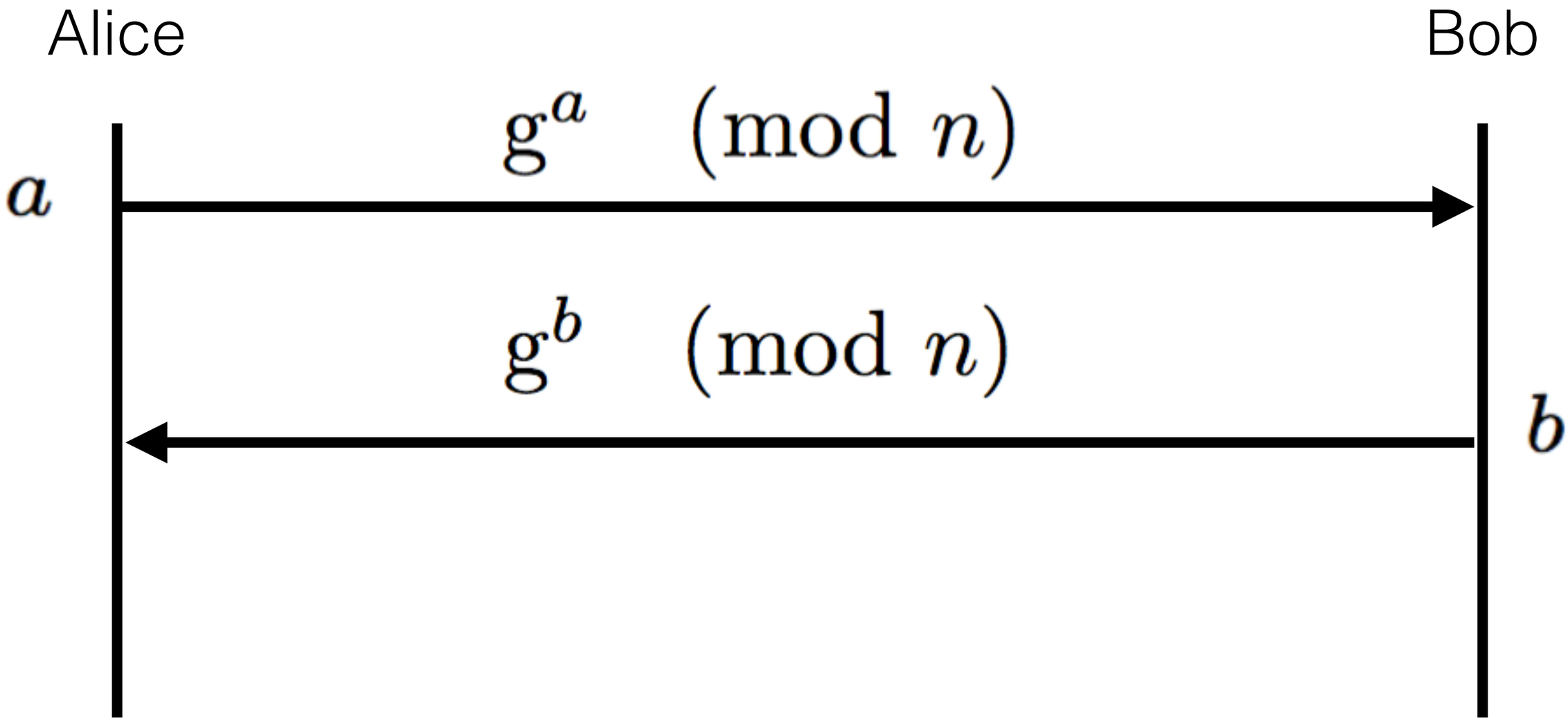
Diffie-Hellman



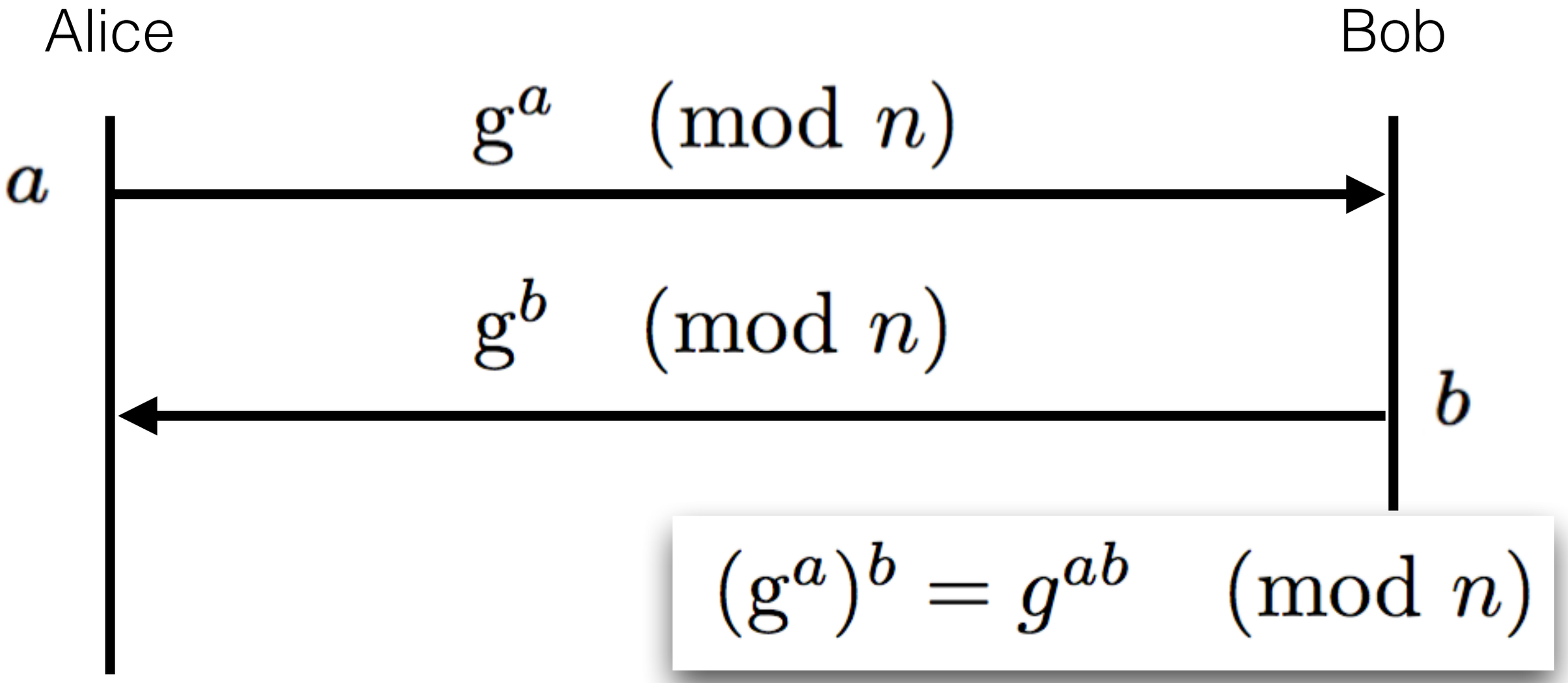
Diffie-Hellman



Diffie-Hellman



Diffie-Hellman



Group Theory

$$\mathrm{g},\ \mathrm{g}^2, g^3, g^4, \ldots \pmod{n}$$

Group Theory

$$\mathrm{g},\ \mathrm{g}^2, g^3, g^4, \ldots \pmod n$$

Alice's $\mathrm{g}^a \pmod n$

Group Theory

$$\mathrm{g},\ \mathrm{g}^2, g^3, g^4, \cdots \pmod{n}$$

$$\cdots, g^{\varphi(n)} = 1$$

Group Theory

$$\mathrm{g},\ \mathrm{g}^2, g^3, g^4, \cdots \pmod{n}$$

$$\cdots, g^{\varphi(n)} = 1, g^{\varphi(n)+1} = g$$

Group Theory

$$\mathrm{g},\ \mathrm{g}^2, g^3, g^4, \cdots \pmod n$$

$$\cdots, g^{\varphi(n)} = 1, g^{\varphi(n)+1} = g, g^2, \cdots \pmod n$$

Group Theory

$$\mathrm{g},\ \mathrm{g}^2, g^3, g^4, \cdots \pmod n$$

$$\cdots, g^{\varphi(n)} = 1, g^{\varphi(n)+1} = g, g^2, \cdots \pmod n$$

$$\varphi(n) = \begin{cases} n-1 \text{ if n prime} \\ \end{cases}$$

Group Theory

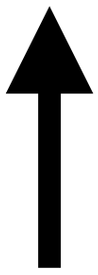
$$\mathrm{g},\ \mathrm{g}^2, g^3, g^4, \cdots \pmod n$$

$$\cdots, g^{\varphi(n)} = 1, g^{\varphi(n)+1} = g, g^2, \cdots \pmod n$$

$$\varphi(n) = \begin{cases} n-1 \text{ if n prime} \\ (p-1)(q-1) \text{ if } n = pq \end{cases}$$

Group Theory

$$g, g^2, g^3, g^4, g^5, g^6, g^7, \cdots, g^{\varphi(n)}$$



Group Theory

$$g, g^2, g^3, g^4, g^5, g^6, g^7, \cdots, g^{\varphi(n)}$$

Group Theory

$$, g^2, \quad , g^4, \quad , g^6, \quad , \cdots ,$$

Group Theory

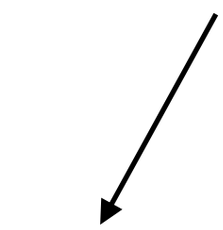
$$\varphi(p) = p - 1 = \quad p_1 \quad \times \cdots \times p_k$$

Known attacks against **DH**

$$g^a \pmod{n}$$

Known attacks against **DH**

$$g^a \pmod{n}$$



a

Known attacks against **DH**

- Trial Multiplication

$$g^a \pmod{n}$$

a

Known attacks against **DH**

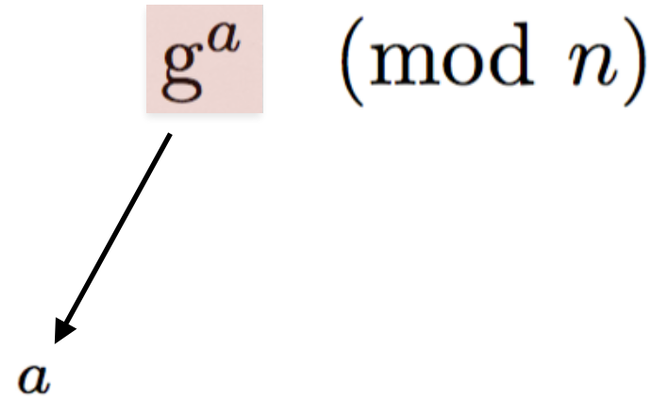
- Trial Multiplication
- SNFS, GNFS

$$g^a \pmod n$$

a

Known attacks against **DH**

- Trial Multiplication
- SNFS, GNFS
- Shank's BSGS, **Pollard Rho** & Kangaroo, …



Known attacks against **DH**

- Trial Multiplication
- SNFS, GNFS
- Shank's BSGS, **Pollard Rho** & Kangaroo, …
- Small subgroup attacks (active)

$$g^a \pmod n$$

a

Known attacks against **DH**

- Trial Multiplication
- SNFS, GNFS
- Shank's BSGS, **Pollard Rho** & Kangaroo, …
- Small subgroup attacks (active)
- **Pohlig-Hellman** (passive)

$$g^a \pmod n$$

$$a$$

Pohlig-Hellman

$$g^a \pmod{n}$$

$$\downarrow$$

$$a$$

Pohlig-Hellman

$$(\mathrm{g}^a)^k \pmod{n}$$

$$a \pmod{l}$$

Prime groups

$$\varphi(p) = p - 1 = p_1 \times \cdots \times p_k$$

$$y = g^x \pmod{p}$$

Prime groups

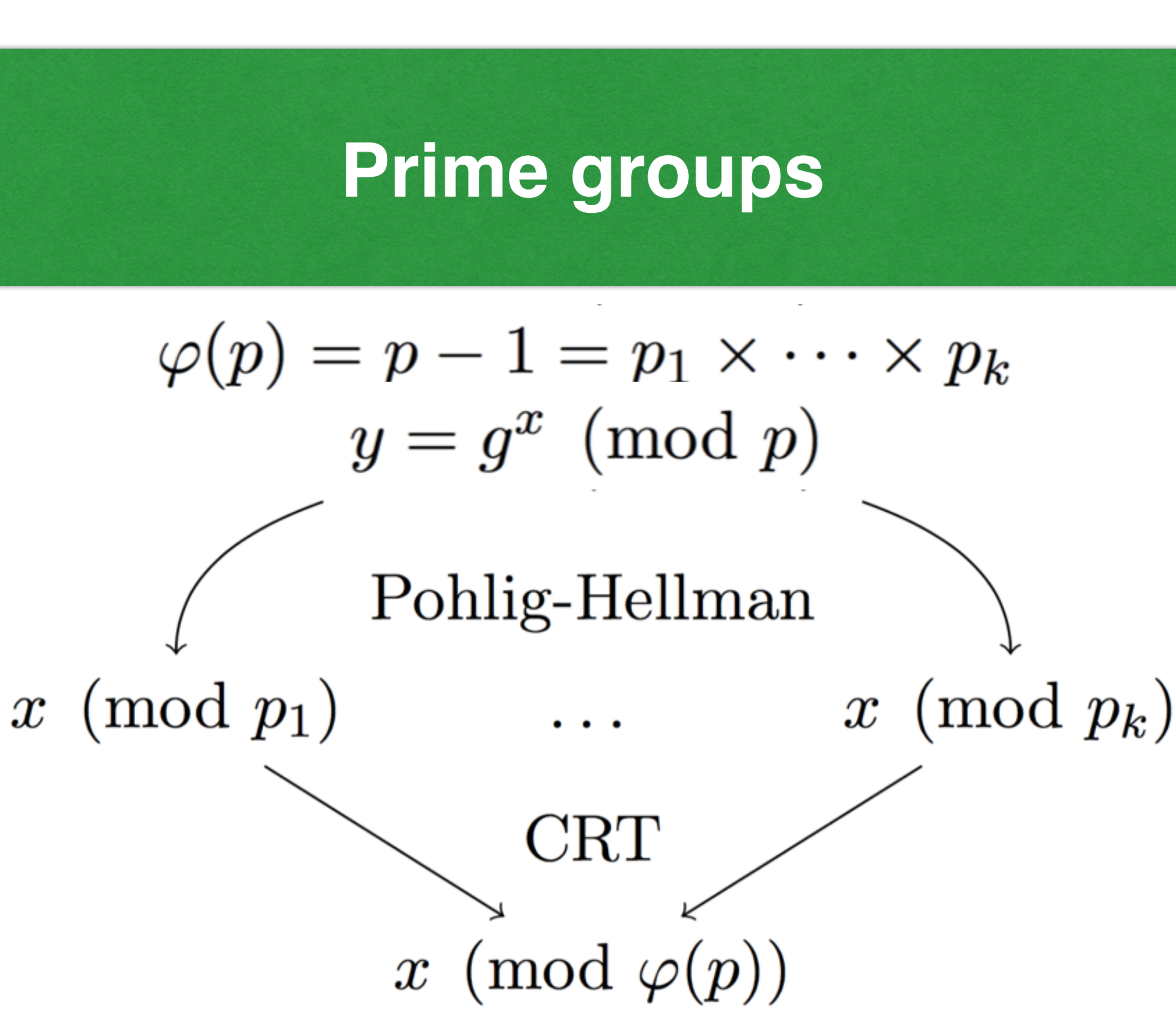
$$\varphi(p) = p - 1 = p_1 \times \cdots \times p_k$$

$$y = g^x \pmod{p}$$

Prime groups

$$\varphi(p) = p - 1 = p_1 \times \cdots \times p_k$$

$$y = g^x \pmod{p}$$



Prime groups

$$\varphi(p) = p - 1 = p_1 \times \cdots \times p_k$$

$$y = g^x \pmod{p}$$

Pohlig-Hellman

$$x \pmod{p_1} \quad \ldots \quad x \pmod{p_k}$$

CRT

$$x \pmod{\varphi(p)}$$

CM-HSO

Composite Modulus with a Hidden Smooth Order

$$\varphi(n) = (p-1) \times (q-1)$$

CM-HSO

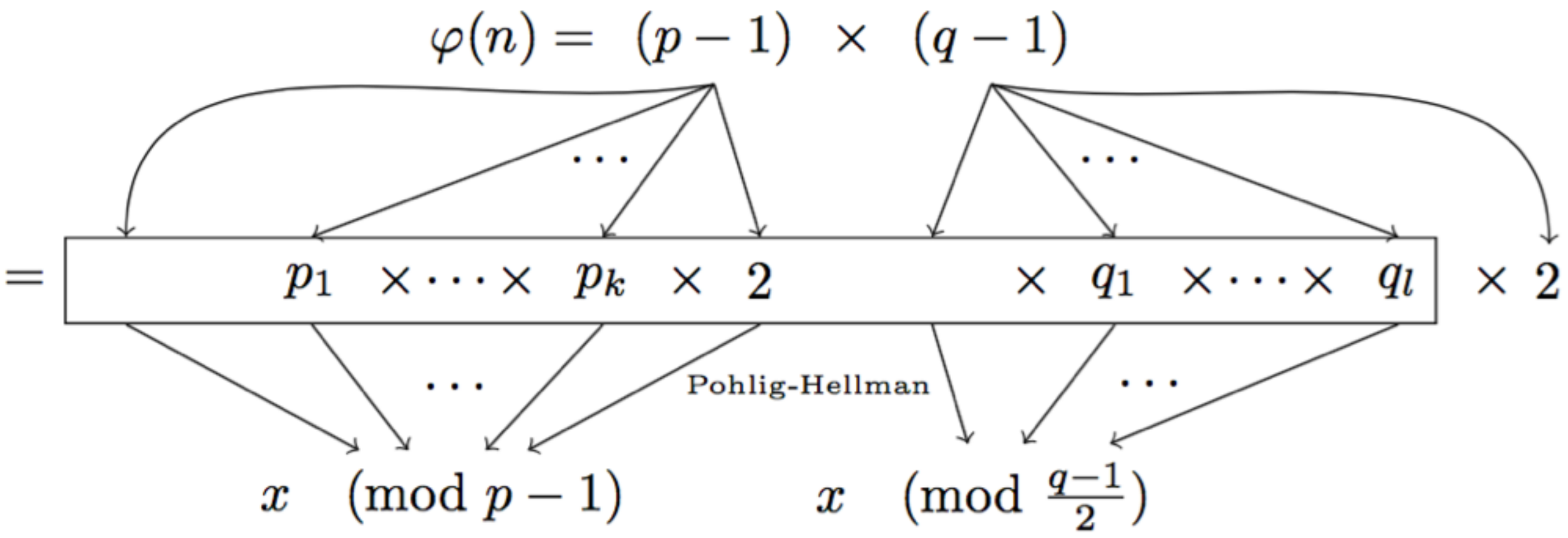
Composite Modulus with a Hidden Smooth Order

$$\varphi(n) = (p-1) \times (q-1)$$

$$= \boxed{p_1 \times \cdots \times p_k \times 2 \times q_1 \times \cdots \times q_l} \times 2$$

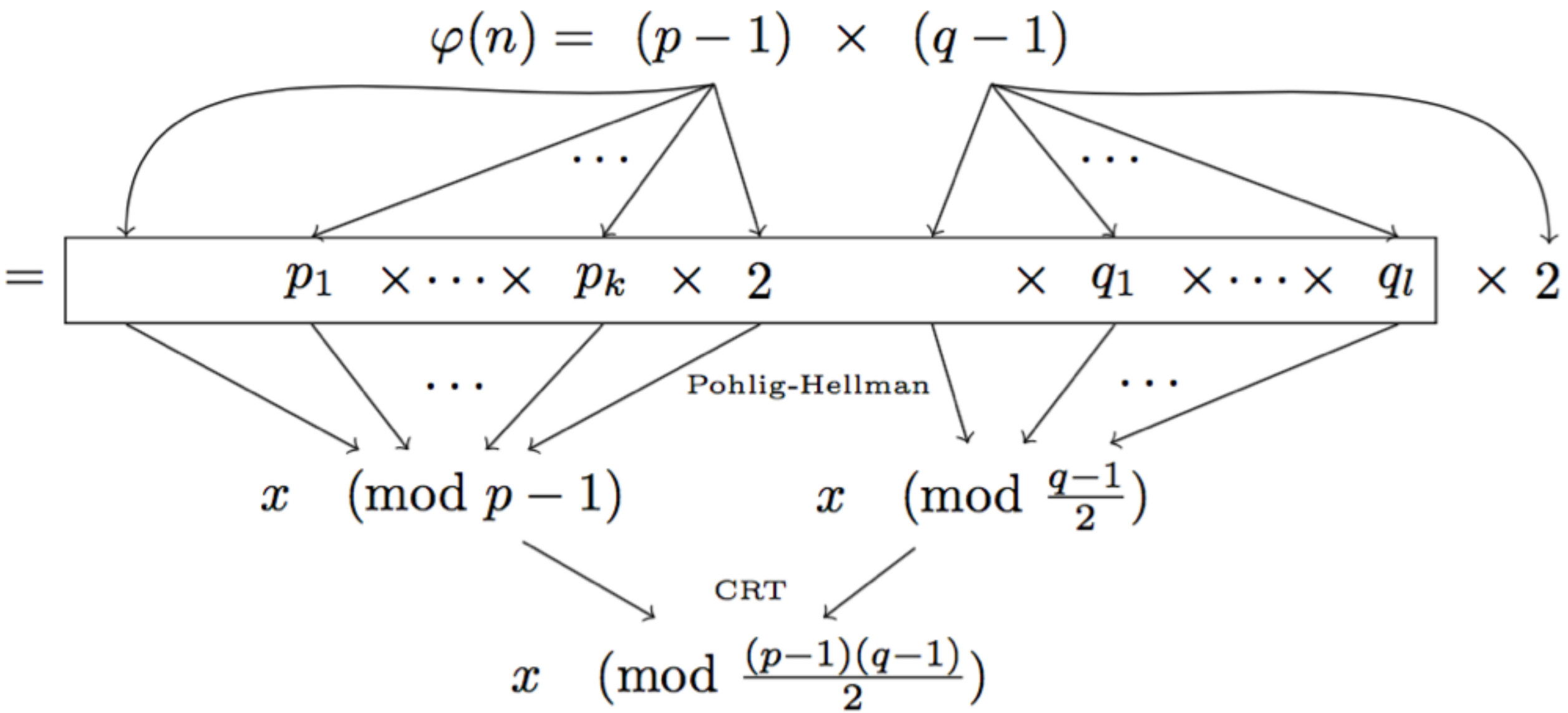
CM-HSO

Composite Modulus with a Hidden Smooth Order



CM-HSO

Composite Modulus with a Hidden Smooth Order



src — _zsh_tmux_plugin_run — tmux

```
File Edit Options Buffers Tools C Help
   {
      static unsigned char dh1024_p[] = {
   0x4b,0x60,0xd1,0x11,0xa2,0x1c,0xa8,0x31,0x43,0xe8,0x5c,0x0b,
   0xbf,0xf8,0xbb,0xcf,0x9e,0xfb,0xbc,0xe9,0x61,0x32,0x2c,0xfe,
   0xf9,0x3d,0x68,0x08,0x9a,0xa2,0x25,0xa9,0x78,0x13,0xb7,0x9f,
   0xc3,0xa4,0x33,0xb0,0x50,0x6c,0x4e,0xea,0xcd,0xbf,0x98,0x3e,
   0x25,0x56,0x23,0x79,0x49,0xbe,0x1b,0x12,0xd0,0xdd,0xfe,0x05,
   0xfb,0x93,0xdc,0xca,0x4f,0xed,0xbc,0xf0,0x35,0x01,0x55,0x0d,
   0x70,0xc6,0xb8,0xe8,0xbe,0x6a,0xba,0xc3,0x72,0xa8,0x30,0x12,
   0x10,0xab,0xfa,0xab,0x0c,0xdc,0xa8,0x98,0xf7,0x1d,0x85,0xde,
   0xb9,0xec,0x16,0x45,0x05,0x51,0x05,0x89,0xa1,0xe4,0xaf,0x1f,
   0x70,0x76,0x25,0xde,0xac,0x24,0x99,0x7d,0x09,0x4c,0xe3,0xb0,
   0xc4,0x18,0x13,0xc1
      };
      static unsigned char dh1024_g[] = {
   0x02,
      };
      DH *dh;
-UU-:**--F1  xio-openssl.c   57% L924  Git-3ee5ac5  (C/l Abbrev) --

[0] <r_generatorZ 2:emacs*> "dhcp-101.chi.matasano" 11:45 03-May-166
```

src — _zsh_tmux_plugin_run — tmux

```
File Edit Options Buffers Tools C Help
   {
      static unsigned char dh1024_p[] = {
   0xCC,0x17,0xF2,0xDC,0x96,0xDF,0x59,0xA4,0x46,0xC5,0x3E,0x0E,
   0xB8,0x26,0x55,0x0C,0xE3,0x88,0xC1,0xCE,0xA7,0xBC,0xB3,0xBF,
   0x16,0x94,0xD8,0xA9,0x45,0xA2,0xCE,0xA9,0x5B,0x22,0x25,0x5F,
   0x92,0x59,0x94,0x1C,0x22,0xBF,0xCB,0xC8,0xC8,0x57,0xCB,0xBF,
   0xBC,0x0E,0xE8,0x40,0xF9,0x87,0x03,0xBF,0x60,0x9B,0x08,0xC6,
   0x8E,0x99,0xC6,0x05,0xFC,0x00,0xD6,0x6D,0x90,0xA8,0xF5,0xF8,
   0xD3,0x8D,0x43,0xC8,0x8F,0x7A,0xBD,0xBB,0x28,0xAC,0x04,0x69,
   0x4A,0x0B,0x86,0x73,0x37,0xF0,0x6D,0x4F,0x04,0xF6,0xF5,0xAF,
   0xBF,0xAB,0x8E,0xCE,0x75,0x53,0x4D,0x7F,0x7D,0x17,0x78,0x0E,
   0x12,0x46,0x4A,0xAF,0x95,0x99,0xEF,0xBC,0xA6,0xC5,0x41,0x77,
   0x43,0x7A,0xB9,0xEC,0x8E,0x07,0x3C,0x6D,
      };
      static unsigned char dh1024_g[] = {
   0x02,
      };
      DH *dh;
-UU-:----F1  xio-openssl.c   57% L923  Git-3ee5ac5  (C/l Abbrev) --

[0] <r_generatorZ 2:emacs*> "dhcp-101.chi.matasano" 11:43 03-May-166
```

```
vagrant@proxy:/vagrant/shared$ go build proxy.go attack.go && sudo ./proxy -l 19
2.168.0.66:6666 -r 192.168.0.50:4433
```

```
vagrant@server:~$ sudo socat openssl-listen:4433,verify=0,cert
=server.pem,key=server.key,cipher=DHE-RSA-AES128-SHA256,reusea
ddr -
```

```
vagrant@client:~/shared$ socat - openssl:192.168.0.66:6666,ver
ify=0,reuseaddr
```

```
[0] 0:..deBasedCrypto- 1:../github_socat  2:vagrant*                    "dhcp-101.chi.matasano" 12:12 27-Jun-161
```

https://github.com/mimoo/**Diffie-Hellman_Backdoor**

Detect and Protect

- Check for prime modulus

Detect and Protect

- Check for prime modulus
- Better: check for **safe prime** modulus

Detect and Protect

- Check for prime modulus
- Better: check for **safe prime** modulus
- Google Chrome deprecating DHE (-> ECDHE)

END

how many VPN/libraries/closed-source products are **backdoored**?

END

how many VPN/libraries/closed-source products are **backdoored**?

what about **ECDHE**?

twitter.com/**lyon01_david**