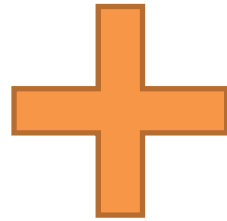


Backdoors in Cryptography

Claudio Orlandi
Associate Professor, Computer Science
Aarhus University

Cryptography

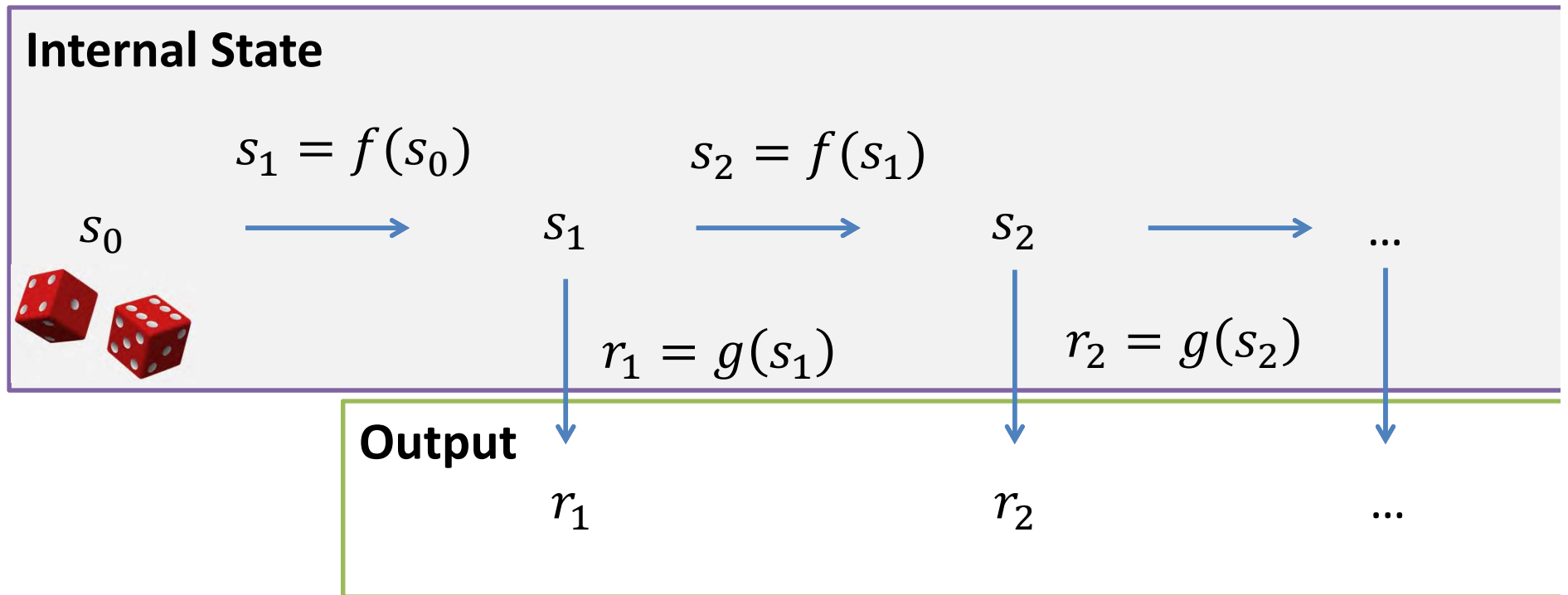
**Computational
hardness**



Unpredictability



Pseudorandom generator



“Looks like truly random outputs”

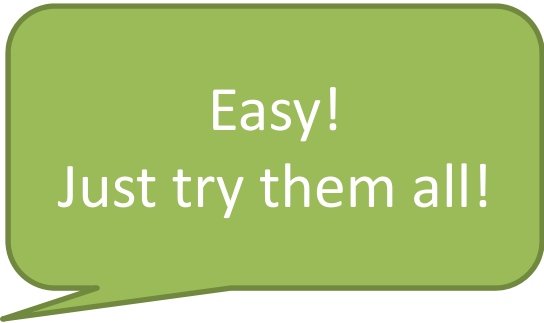
Discrete Logarithm Problem

- Logarithm: find x such that

$$3^x = 81$$

- Discrete logarithm problem

$$3^x \bmod 47 = 34$$



Easy!
Just try them all!

Discrete Logarithm Problem

- Logarithm: find x such that

$$3^x = 81$$

- Discrete logarithm problem

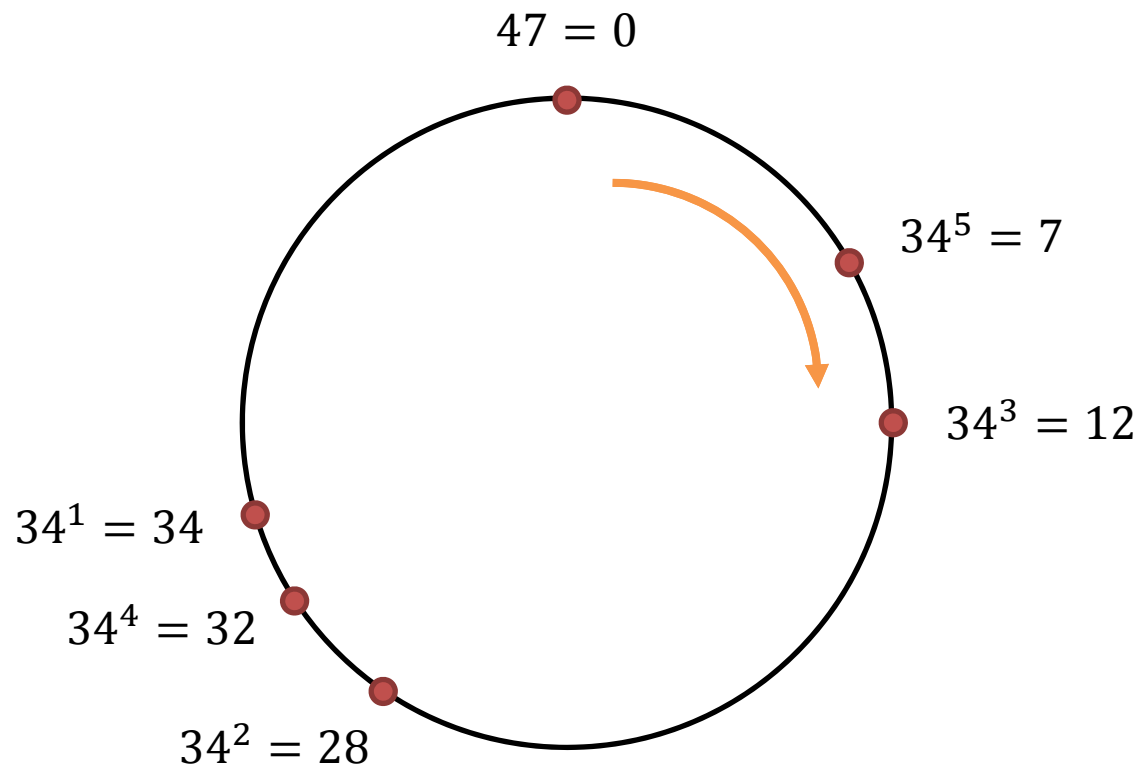
$$3^x \bmod 4 \dots 7 = 3 \dots 4$$

1000 digits (3000 bits)



Hard!

Computing *mod* 47



$$34^2 = 1156 = 47 \cdot 24 + \textcircled{28} \quad \Rightarrow \quad 34^2 \text{ mod } 47 = 28$$

Dual_EC (Simplified)

- Two hardwired parameters

$$(P, Q)$$

- Initial (truly) random state

$$s_0$$

- Compute next state

$$s_{i+1} = P^{s_i} \bmod N$$

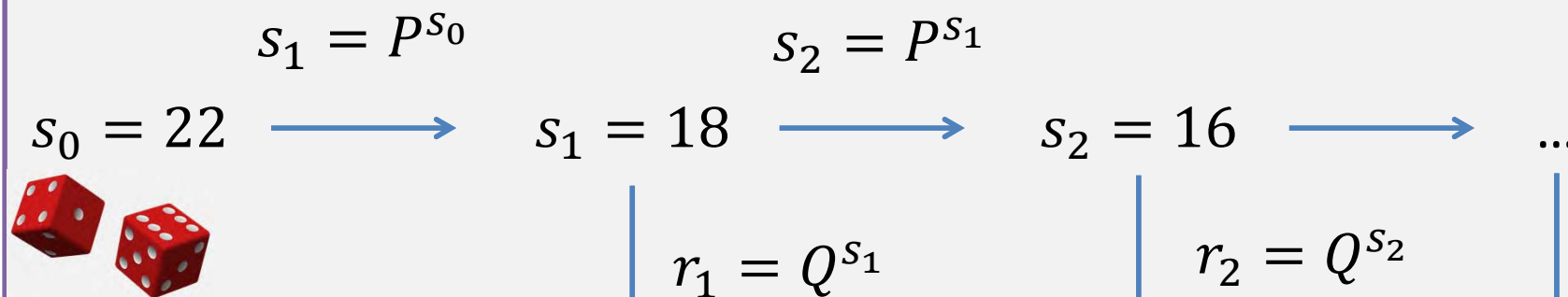
- Compute output

$$r_i = Q^{s_i} \bmod N$$

mod 47
P=34
Q=3

Dual_EC (Simplified)

Internal State



Output

$$r_1 = 6$$

$$r_2 = 32$$

\dots

mod 47

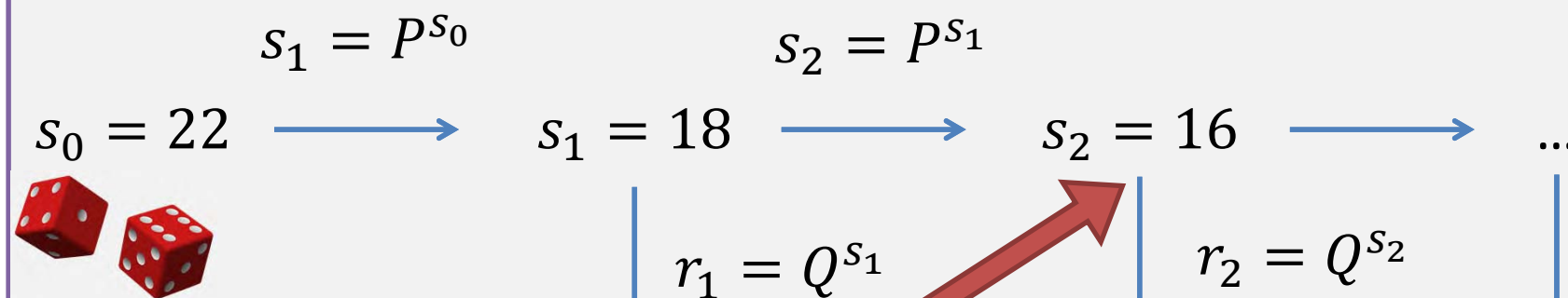
P=34

Q=3

x=7

DUAL_EC Backdoor(Simplified)

Internal State



Output

$$r_1 = 6$$

$$r_2 = 32$$

Given x such that

$$P = Q^x$$

Can recover internal state

$$s_2 = r_1^x$$

DUAL_EC **Backdoor** (Simplified)

The user

- Two parameters
 (P, Q)
- Compute next state
 $s_{i+1} = P^{s_i} \bmod N$
- Compute next output
 $r_i = Q^{s_i} \bmod N$

The attacker

- Keep x such that
 $P = Q^x \bmod N$
- Observe any output
 r_i
- Compute next state
 $s_{i+1} = r_i^x \bmod N$
- Predict all future outputs!

$$s_{i+1} = P^{s_i} = (Q^x)^{s_i} = (Q^{s_i})^x = r_i^x \bmod N$$

HTTPS (Simplified)



Choose random r_1

r_1

...

Choose random r_2

$Enc(pk, r_2)$

$K = F(r_1, r_2, \dots)$

$K = F(r_1, r_2, \dots)$

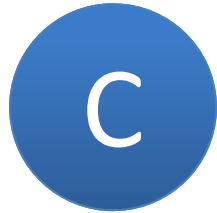


Knows r_1

Does not know r_2

→ Cannot compute K

HTTPS with **Backdoor** (Simplified)



Choose random r_1

Using Dual_EC

r_1

...

Choose random r_2

Using Dual_EC

$Enc(pk, r_2)$

$K = F(r_1, r_2, \dots)$



$K = F(r_1, r_2, \dots)$



Knows r_1 **Knows x**

~~Does not know r_2~~ **Predicts r_2**

~~→ Cannot compute K~~ **Computes K**

- Unless you choose your own parameters, DUAL_EC is a really bad PRNG.
- If you use parameters (P,Q) chosen by an adversary, you grant the adversary the power to eavesdrop virtually any secure connection you can establish over the internet.
- *But this would never happen. Right?*

Dual_EC : a brief history

- 2007
 - Dual_EC standardized by NIST with fixed parameters P,Q
 - The standard is criticized at CRYPTO 2007

Conclusion

- WHAT WE ARE NOT SAYING:
NIST intentionally put a back door in this PRNG
- WHAT WE ARE SAYING:
The prediction resistance of this PRNG (as presented in NIST SP800-90) is dependent on solving one instance of the elliptic curve discrete log problem.
(And we do not know if the algorithm designer knew this before hand.)

- 2013

- Snowden reveals existence of Bullrun program

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.



TOP SECRET STRAP1

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

PTD "We penetrate targets' defences."

This information is exempt from automatic release under the provisions of the Official Information Act 2007 and may also be exempt from disclosure under other UK Freedom of Information legislation. This information is exempt from automatic release under the provisions of the Official Information Act 2007 and may also be exempt from disclosure under other UK Freedom of Information legislation. © Crown Copyright. All rights reserved.

TOP SECRET STRAP1

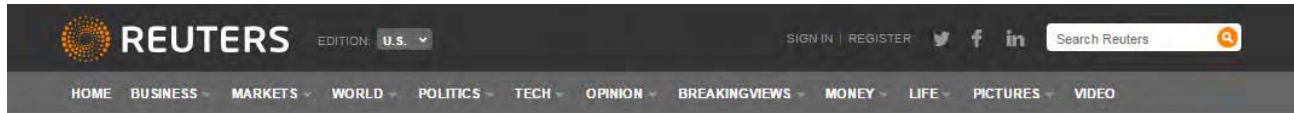
BULLRUN Bottom Line

- Groundbreaking capabilities
- Extremely fragile
- Do not ask about or speculate on sources or methods underpinning BULLRUN successes
- Indoctrination required for access to secure COI

PTD "We penetrate targets' defences."

This information is exempt from automatic release under the provisions of the Official Information Act 2007 and may also be exempt from disclosure under other UK Freedom of Information legislation. This information is exempt from automatic release under the provisions of the Official Information Act 2007 and may also be exempt from disclosure under other UK Freedom of Information legislation. © Crown Copyright. All rights reserved.

- 2013
 - RSA accused of accepting 10M\$ to adopt Dual_EC in their products



Technology | Mon Mar 31, 2014 4:27pm EDT

Related: ELECTION 2016, POLITICS, TECH

Exclusive: NSA infiltrated RSA security more deeply than thought - study

SAN FRANCISCO | BY JOSEPH MENN



A sign marks the entrance to RSA's facility in Bedford, Massachusetts March 28, 2014.
REUTERS/BRIAN SNYDER

Security industry pioneer RSA adopted not just one but two encryption tools developed by the U.S. National Security Agency, greatly increasing the spy agency's ability to eavesdrop on some Internet communications, according to a team of academic researchers.

Reuters reported in December that the NSA had paid RSA \$10 million to make a now-discredited cryptography system the default in software used by a wide range of Internet and computer security programs. The system, called Dual Elliptic Curve, was a random number generator, but it had a deliberate flaw - or "back door" - that allowed the NSA to crack the encryption.

- 2014

- NIST investigates

Subject: [Fwd: RE: Minding our Ps and Qs in Dual_EC]
Date: Wednesday, October 27, 2004 at 12:09:25 PM Eastern Daylight Time
From: John Kelsey
To: Larry.basham@nist.gov

----- Original Message -----
Subject: RE: Minding our Ps and Qs in Dual_EC
From: "Don Johnson" <DJohnson@cygnacom.com>
Date: Wed, October 27, 2004 11:42 am
To: "John Kelsey" <john.kelsey@nist.gov>

John,
P=G.

Q is (in essence) the public key for some random private key.

It could also be generated like another canonical G, but NSA kyboshed this idea, and I was not allowed to publicly discuss it, just in case you may think of going there.

Don B. Johnson

-----Original Message-----
From: John Kelsey fmail to:john.kelsey@nist.gov]
Sent: Wednesday, October 27, 2004 11:17 AM
To: Don Johnson
Subject: Minding our Ps and Qs in Dual_EC

Do you know where Q comes from in Dual_EC_DRBG?

Thanks,
-John

- 2015

- Juniper (who had been using Dual_EC but with their own P,Q), discovers that in 2012 someone hacked their servers and changed the constants.

DJIA ▲ 17024.47 0.10% Nasdaq ▼ 4701.45 -0.33% U.S. 10 Yr ▼ -9/32 Yield 1.908% Crude Oil ▲ 37.17 3.48% Euro ▼ 1.0976 -0.27%

THE WALL STREET JOURNAL.

Subscribe Now | Sign In
SPECIAL OFFER: JOIN NOW

Home World U.S. Politics Economy Business Tech Markets **Opinion** Arts Life Real Estate Q

REVIEW & OUTLOOK
The GOP Race Isn't Over

REVIEW & OUTLOOK
Erdogan's Press Assault

REVIEW & OUTLOOK
Vermont Invades Your Kitchen

OPINION | COMMENTARY

The Data Breach You Haven't Heard About

Foreign hackers may be reading encrypted U.S. government communications, yet basic information about what happened still isn't available.



PHOTO: GETTY IMAGES/IKON IMAGES

Most

- 1.
- 2.
- 3.
- 4.
- 5.

A security breach recently discovered at software developer **Juniper Networks** has U.S. officials worried that foreign hackers have been reading the encrypted communications of U.S. government agencies for the past three years. Yet compared with the uproar over the Office of Personnel Management breach, first disclosed last June, this recent breach has gone largely unnoticed.

On Dec. 17 the California-based Juniper Networks announced that an unauthorized backdoor had been placed in its ScreenOS software, and a breach was possible since 2013. This allowed an outside actor to monitor network traffic, potentially decrypt information, and even take control of firewalls. Days later the company provided its clients—which include various U.S. intelligence entities—with an “emergency security patch” to close the backdoor.

2016

“We cannot build a backdoor that only works for a particular type of government, or only in the presence of a particular court order.”

The screenshot shows the top of a Washington Post article. The header includes the search icon, 'Sections' menu, and the newspaper's name. Below the header are social media sharing icons for Facebook, Twitter, Google+, Email, and a '+ More' option. The article is categorized under 'PostEverything'. The main title is 'Why you should side with Apple, not the FBI, in the San Bernardino iPhone case', with a subtitle 'Either everyone gets security, or no one does.' Below the title are icons for font size (A), print, 929 comments, 'Save for Later', and 'Reading List'. The author is identified as Bruce Schneier, with a bio stating he is a security technologist and CTO of Resilient Systems, Inc., and his latest book is 'Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.' A 'Follow @schneierblog' button is also present. The main image shows a hand holding a smartphone. To the right, there are partial views of other article thumbnails, including one about Rubio's campaign and another about Donald Trump.

Thanks!
Questions?