



Norwegian University of
Science and Technology

LEGACY CRYPTO 2: ATTACKS ON TLS

TTM4205 – Lecture 6

Tjerand Silde

05.09.2025

Contents

Announcements

Legacy Crypto

Legacy PKC

Attacks on TLS

Backdoors

Contents

Announcements

Legacy Crypto

Legacy PKC

Attacks on TLS

Backdoors

Reference Group Meeting

We now have two reference group members:

- ▶ Tom Chauvier (tomchau), exchange student
- ▶ Jo Remvik (jo.v.remvik), MTKOM

We prefer to have additional members from MSTCNNS and SECCLO.

Contents

Announcements

Legacy Crypto

Legacy PKC

Attacks on TLS

Backdoors

Legacy Crypto is...

- ▶ Old and outdated crypto
- ▶ Insecure, weakened, or flawed crypto
- ▶ Crypto regulated by export control
- ▶ Potentially backdoored crypto
- ▶ Key escrow and surveillance
- ▶ Downgradable crypto protocols

Two Categories

Secret Key Crypto

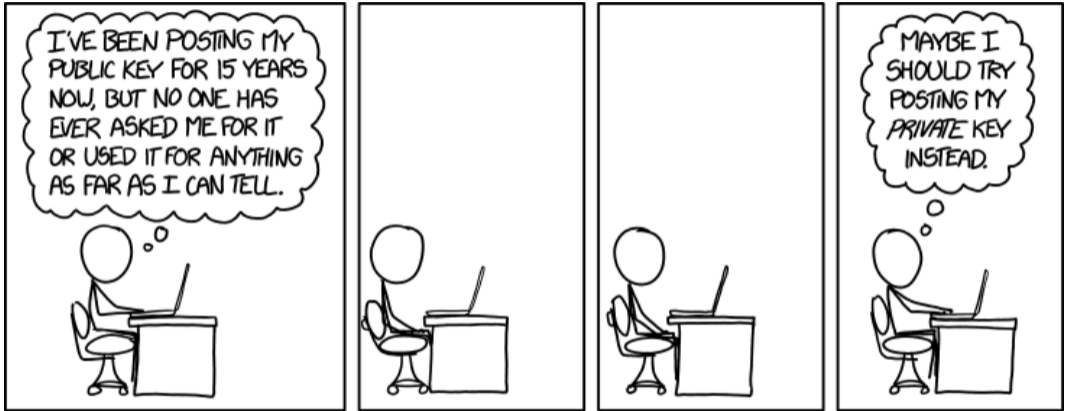
Public Key Crypto

Today

Secret Key Crypto

Public Key Crypto

Public Key Crypto



Contents

Announcements

Legacy Crypto

Legacy PKC

Attacks on TLS

Backdoors

Legacy Ciphers

While we have attacks against symmetric key ciphers making them obsolete, we do not have groundbreaking attacks against legacy public key ciphers.

However, we need to be careful when setting parameters and composing different schemes in more complex protocols.

Here are some examples...

Weak DH

Weak DH

- ▶ Improved discrete log → Must use larger keys

Weak DH

- ▶ Improved discrete log → Must use larger keys
- ▶ Non-prime group \mathbb{Z}_q^* → Leaks Legendre symbol of m
 - ▶ computing DL depends on largest prime factor $p|(q-1)$
 - ▶ messages with different Legendre symbol → break DDH
 - ▶ need generator g to be of order p for CPA security

Weak DH

- ▶ Improved discrete log → Must use larger keys
- ▶ Non-prime group \mathbb{Z}_q^* → Leaks Legendre symbol of m
 - ▶ computing DL depends on largest prime factor $p|(q-1)$
 - ▶ messages with different Legendre symbol → break DDH
 - ▶ need generator g to be of order p for CPA security
- ▶ Supersingular curves → Can break Decisional DH

Weak DH

- ▶ Improved discrete log → Must use larger keys
- ▶ Non-prime group \mathbb{Z}_q^* → Leaks Legendre symbol of m
 - ▶ computing DL depends on largest prime factor $p|(q-1)$
 - ▶ messages with different Legendre symbol → break DDH
 - ▶ need generator g to be of order p for CPA security
- ▶ Supersingular curves → Can break Decisional DH
- ▶ Choose safe curves? → Standardized P-256, X25519, ...



Elliptic Curve Cryptography in Practice

Joppe W. Bos¹, J. Alex Halderman², Nadia Heninger³, Jonathan Moore, Michael Naehrig¹,
and Eric Wustrow²

¹ Microsoft Research

² University of Michigan

³ University of Pennsylvania

Figure: <https://eprint.iacr.org/2013/734.pdf>

Weak RSA

Weak RSA

- ▶ Improved factoring → Must use larger keys

Weak RSA

- ▶ Improved factoring \rightarrow Must use larger keys
- ▶ If $d < \frac{1}{3}N^{1/4} \rightarrow$ Wiener's attack to recover d

Weak RSA

- ▶ Improved factoring \rightarrow Must use larger keys
- ▶ If $d < \frac{1}{3}N^{1/4} \rightarrow$ Wiener's attack to recover d
- ▶ Small key $e \rightarrow$ Håstad's attack to recover m

Weak RSA

- ▶ Improved factoring → Must use larger keys
- ▶ If $d < \frac{1}{3}N^{1/4}$ → Wiener's attack to recover d
- ▶ Small key e → Håstad's attack to recover m
- ▶ Several attacks by Don Coppersmith (NSA since 2005)
 - ▶ Efficient factoring when e is very small
 - ▶ Message recovery against short padding
 - ▶ Factoring given partial bits of p

Weak RSA

- ▶ Improved factoring → Must use larger keys
- ▶ If $d < \frac{1}{3}N^{1/4}$ → Wiener's attack to recover d
- ▶ Small key e → Håstad's attack to recover m
- ▶ Several attacks by Don Coppersmith (NSA since 2005)
 - ▶ Efficient factoring when e is very small
 - ▶ Message recovery against short padding
 - ▶ Factoring given partial bits of p
- ▶ If $e < \sqrt{N}$, given $\frac{1}{4} \log_2 N$ bits of d → Can reconstruct d



Weak RSA

- ▶ Improved factoring → Must use larger keys
- ▶ If $d < \frac{1}{3}N^{1/4}$ → Wiener's attack to recover d
- ▶ Small key e → Håstad's attack to recover m
- ▶ Several attacks by Don Coppersmith (NSA since 2005)
 - ▶ Efficient factoring when e is very small
 - ▶ Message recovery against short padding
 - ▶ Factoring given partial bits of p
- ▶ If $e < \sqrt{N}$, given $\frac{1}{4} \log_2 N$ bits of d → Can reconstruct d
- ▶ PKCS 1 padding → Bleichenbacher's padding attack

Twenty Years of Attacks on the RSA Cryptosystem

Dan Boneh
dabo@cs.stanford.edu

Figure: <https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf>

RSA Challenges

Challenge Name	Digits	Bits	Date Factored	Factored by
RSA-100	100	330	Apr 1, 1991	A. K. Lenstra
RSA-110	110	364	Apr 14, 1992	A. K. Lenstra and M.S. Manasse
RSA-120	120	397	Jul 9, 1993	T. Denny et al.
RSA-130	130	430	Apr 10, 1996	A. K. Lenstra et al.
RSA-140	140	463	Feb 2, 1999	H. te Riele et al.
RSA-150	150	496	Apr 16, 2004	K. Aoki et al.
RSA-155	155	512	Aug 22, 1999	H. te Riele et al.
RSA-160	160	530	Apr 1, 2003	J. Franke et al.
RSA-170	170	563	Dec 29, 2009	D. Bonenberger and M. Krone
RSA-576	174	576	Dec 3, 2003	J. Franke et al.
RSA-180	180	596	May 8, 2010	S. A. Danilov and I. A. Popovyan
RSA-190	190	629	Nov 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	Nov 2, 2005	J. Franke et al.
RSA-200	200	663	May 9, 2005	J. Franke et al.
RSA-210	210	696	Sep 26, 2013	R. Propper
RSA-704	212	704	Jul 2, 2012	S. Bai, E. Thomé and P. Zimmermann
RSA-220	220	729	May 13, 2016	S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann
RSA-230	230	762	Aug 15, 2018	S. S. Gross
RSA-768	232	768	Dec 12, 2009	T. Kleinjung et al.
RSA-240	240	795	Nov 24, 2019	F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann
RSA-250	250	829	Feb 28, 2020	F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann

Table 1. The solved RSA Challenges

Figure: <https://eprint.iacr.org/2021/894.pdf>

Key Sizes

	Parameter	Legacy	Future System Use	
			Near Term	Long Term
Symmetric Key Size	k	80	128	256
Hash Function Output Size	m	160	256	512
MAC Output Size	m	80	128	256
RSA Problem	$\ell(n) \geq$	1024	3072	15360
Finite Field DLP	$\ell(p^n) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512
ECDLP	$\ell(q) \geq$	160	256	512
Pairing	$\ell(q^n) \geq$	1024	3072	15360
	$\ell(p), \ell(q) \geq$	160	256	512

Table 2. Key Size Analysis, where $\ell(\cdot)$ refers to the bit-length of the parameter.

Figure: <https://eprint.iacr.org/2021/894.pdf>

Contents

Announcements

Legacy Crypto

Legacy PKC

Attacks on TLS

Backdoors

Static Finite Field DH

Static Finite Field DH

- ▶ A MitM attack on TLS \leq 1.2 can choose weak ciphers

Static Finite Field DH

- ▶ A MitM attack on TLS \leq 1.2 can choose weak ciphers
- ▶ Export Diffie-Hellman accept 512 bit prime groups

Static Finite Field DH

- ▶ A MitM attack on TLS \leq 1.2 can choose weak ciphers
- ▶ Export Diffie-Hellman accept 512 bit prime groups
- ▶ One week of pre-computation \rightarrow DL takes 1 min

Static Finite Field DH

- ▶ A MitM attack on TLS \leq 1.2 can choose weak ciphers
- ▶ Export Diffie-Hellman accept 512 bit prime groups
- ▶ One week of pre-computation \rightarrow DL takes 1 min
- ▶ 2015: two 1024 groups break 18% HTTPS and 26% SSH

Logjam Attack

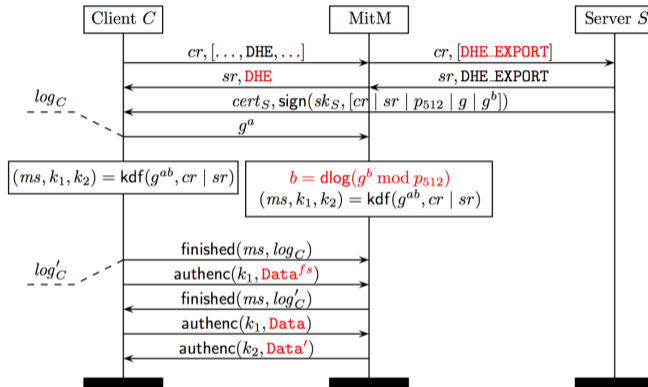


Figure: <https://weakdh.org/imperfect-forward-security.pdf>

Old Attacks on TLS

RC4

- Roos's Bias 1995
- Fluhrer, Martin & Shamir 2001
- Klein 2005
- Combinatorial Problem 2001
- Royal Holloway 2013
- Bar-mitzvah 2015
- NOMORE 2015

RSA-PKCS#1 v1.5 Encryption

- Bleichenbacher 1998
- Jager 2015
- DROWN 2016

Renegotiation

- Marsh Ray Attack 2009
- Renegotiation DoS 2011
- Triple Handshake 2014

3DES

- Sweet32

AES-CBC

- Vaudenay 2002
- Boneh/Brumley 2003
- BEAST 2011
- Lucky13 2013
- POODLE 2014
- Lucky Microseconds 2015

Compression

- CRIME 2012

MD5 & SHA1

- SLOTH 2016
- SHAttered 2017

Figure: https://owasp.org/www-chapter-london/assets/slides/OWASPLondon20180125_TLSv1.3_Andy_Brodie.pdf

Downgrade Attacks on TLS

TLS: a long year of downgrade attacks

- POODLE TLS 1.2 → SSLv3 [Dec'14]
- FREAK RSA-2048 → RSA-512 [Mar'15]
- **LOGJAM** **DH-2048 → DH-512** **[May'15]**
- BLEICH? RSA-Sign → RSA-Enc [Aug'15]
- **SLOTH** **RSA-SHA256 → RSA-MD5** **[Jan'16]**

Figure: <https://rwc.iacr.org/2016/Slides/Downgrade.pdf>

From TLS 1.2 to 1.3

From TLS 1.2 to 1.3

- ▶ Removed RSA for key exchange

From TLS 1.2 to 1.3

- ▶ Removed RSA for key exchange
- ▶ Removed RC4, 3DES and Camellia

From TLS 1.2 to 1.3

- ▶ Removed RSA for key exchange
- ▶ Removed RC4, 3DES and Camellia
- ▶ Removed MD5 and SHA-1 hash functions

From TLS 1.2 to 1.3

- ▶ Removed RSA for key exchange
- ▶ Removed RC4, 3DES and Camellia
- ▶ Removed MD5 and SHA-1 hash functions
- ▶ Removed AES-CBC encryption mode

From TLS 1.2 to 1.3

- ▶ Removed RSA for key exchange
- ▶ Removed RC4, 3DES and Camellia
- ▶ Removed MD5 and SHA-1 hash functions
- ▶ Removed AES-CBC encryption mode
- ▶ Removed static (EC) Diffie-Hellman

From TLS 1.2 to 1.3

- ▶ Removed RSA for key exchange
- ▶ Removed RC4, 3DES and Camellia
- ▶ Removed MD5 and SHA-1 hash functions
- ▶ Removed AES-CBC encryption mode
- ▶ Removed static (EC) Diffie-Hellman
- ▶ Only standardized groups/curves

New Cipher Suits

TLS 1.3 only allows for 5 different cipher suits:

- ▶ (EC)DHE-AES-128-GCM-SHA256
- ▶ (EC)DHE-AES-256GCM-SHA384
- ▶ (EC)DHE-CHACHA20-POLY1305-SHA256
- ▶ (EC)DHE-AES-128-CCM-SHA256
- ▶ (EC)DHE-AES-128-CCM-8-SHA256

Matthew Green's Blog

- ▶ Standards: <https://blog.cryptographyengineering.com/2011/10/04/how-standards-go-wrong-constructive>
- ▶ Logjam: <https://blog.cryptographyengineering.com/2015/05/22/attack-of-week-logjam>
- ▶ FREAK: <https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa>

Contents

Announcements

Legacy Crypto

Legacy PKC

Attacks on TLS

Backdoors

Dual EC

Dual EC

- ▶ PRNG designed by NSA and standardized by NIST

Dual EC

- ▶ PRNG designed by NSA and standardized by NIST
- ▶ It is provably random from DDH over elliptic curves

Dual EC

- ▶ PRNG designed by NSA and standardized by NIST
- ▶ It is provably random from DDH over elliptic curves
- ▶ The input is a random seed s and two points P, Q

Dual EC

- ▶ PRNG designed by NSA and standardized by NIST
- ▶ It is provably random from DDH over elliptic curves
- ▶ The input is a random seed s and two points P, Q
- ▶ The points P and Q are chosen at random

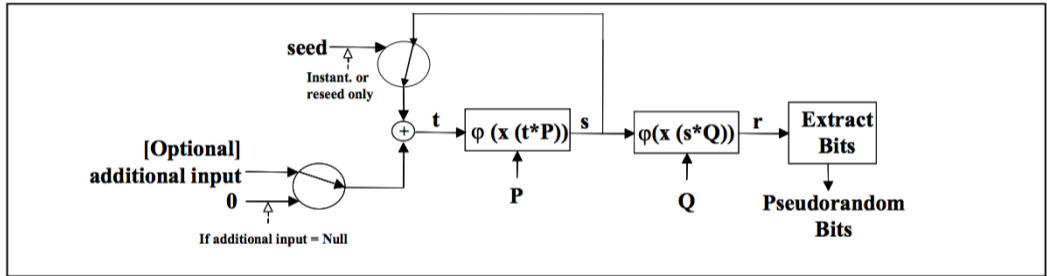
Dual EC

- ▶ PRNG designed by NSA and standardized by NIST
- ▶ It is provably random from DDH over elliptic curves
- ▶ The input is a random seed s and two points P, Q
- ▶ The points P and Q are chosen at random
- ▶ Let $x(P)$ output the x coordinate of the point P

Dual EC

- ▶ PRNG designed by NSA and standardized by NIST
- ▶ It is provably random from DDH over elliptic curves
- ▶ The input is a random seed s and two points P, Q
- ▶ The points P and Q are chosen at random
- ▶ Let $x(P)$ output the x coordinate of the point P
- ▶ Let ϕ be a function that truncates $x(P)$ to bits

Dual EC



A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator

Daniel R. L. Brown* and Kristian Gjøsteen†

February 15, 2007

Figure: <https://eprint.iacr.org/2007/048.pdf>

This is provably biased if you
know $DLOG \log_P Q$

DUAL_EC **Backdoor** (Simplified)

The user	The attacker
<ul style="list-style-type: none">• Two parameters (P, Q)• Compute next state $s_{i+1} = P^{s_i} \bmod N$• Compute next output $r_i = Q^{s_i} \bmod N$	<ul style="list-style-type: none">• 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!

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

Figure: https://www.cs.au.dk/~orlandi/orlandi_backdoors.pdf

Matthew Green's Blog

- ▶ Dual-EC-DRBG: <https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg>
- ▶ RSA warning: <https://blog.cryptographyengineering.com/2013/09/20/rsa-warns-developers-against-its-own>
- ▶ NSA random number: <https://blog.cryptographyengineering.com/2013/12/28/a-few-more-notes-on-nsa-random-number>
- ▶ Juniper backdoor: <https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor>

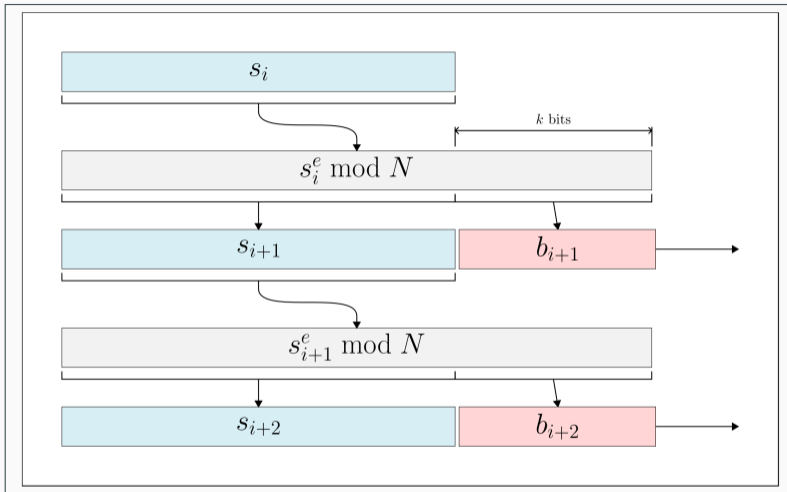


On the Possibility of a Backdoor in the Micali-Schnorr Generator

Hannah Davis¹ Matthew Green² Nadia Heninger¹
Keegan Ryan¹ Adam Suhl¹

Figure: paper: <https://eprint.iacr.org/2023/440.pdf>, talk:
<https://www.youtube.com/watch?v=608NQdTn39Q&t=2629s>, slides:
<https://iacr.org/submit/files/slides/2023/rwc/rwc2023/119/slides.pdf>

Micali-Schnorr?



Unclear how to recover the state using RSA decryption.

Questions?