



Norwegian University of
Science and Technology

LEGACY CRYPTO 1: CRYPTO WARS

TTM4205 – Lecture 5

Tjerand Silde

01.09.2025

Contents

Announcements

Legacy Crypto

Crypto Wars

An Old Cipher

Crypto AG

Newer Ciphers

Newest Ciphers

Contents

Announcements

Legacy Crypto

Crypto Wars

An Old Cipher

Crypto AG

Newer Ciphers

Newest Ciphers

Reference Group

We have 1, but am looking for 2-3 more students to join the reference group. Your feedback is extremely valuable.

Send me an email and/or talk to me in the break :)

Contents

Announcements

Legacy Crypto

Crypto Wars

An Old Cipher

Crypto AG

Newer Ciphers

Newest Ciphers

Legacy Crypto is...

Legacy Crypto is...

- ▶ Old and outdated crypto

Legacy Crypto is...

- ▶ Old and outdated crypto
- ▶ Insecure, weakened, or flawed crypto

Legacy Crypto is...

- ▶ Old and outdated crypto
- ▶ Insecure, weakened, or flawed crypto
- ▶ Crypto regulated by export control

Legacy Crypto is...

- ▶ Old and outdated crypto
- ▶ Insecure, weakened, or flawed crypto
- ▶ Crypto regulated by export control
- ▶ Potentially backdoored crypto

Legacy Crypto is...

- ▶ Old and outdated crypto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

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- ▶ Old and outdated crypto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

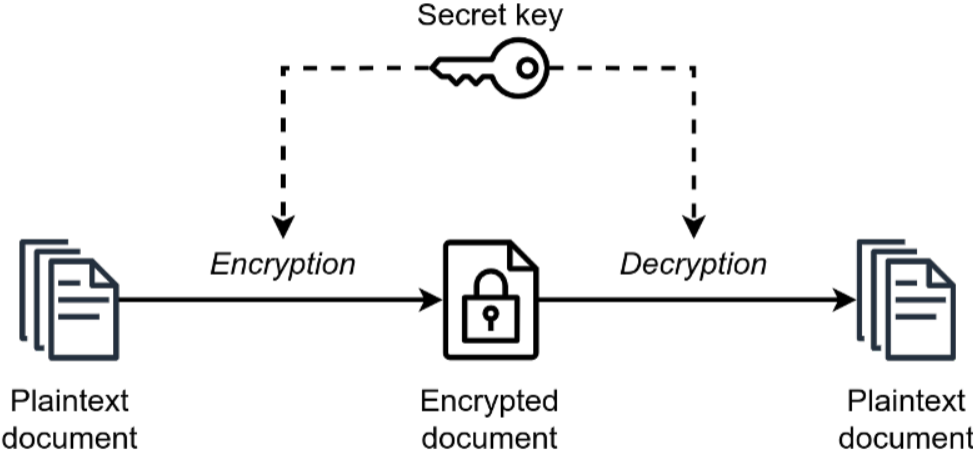
Public Key Crypto

Today

Secret Key Crypto

Public Key Crypto

Secret Key Crypto



Contents

Announcements

Legacy Crypto

Crypto Wars

An Old Cipher

Crypto AG

Newer Ciphers

Newest Ciphers

Crypto Wars

Essentially 30+ year ongoing debate between policymakers and technologists about encryption and surveillance

Typically portrayed as "Safety" vs. "Privacy" to get "Security"

Crypto War I

Crypto War I

- ▶ The 1990s: Wire-tapping vs. cryptography

Crypto War I

- ▶ The 1990s: Wire-tapping vs. cryptography
- ▶ AT&T phone calls encrypted with DH and DES

Crypto War I

- ▶ The 1990s: Wire-tapping vs. cryptography
- ▶ AT&T phone calls encrypted with DH and DES
- ▶ The Clipper-chip and key escrow (broken)

Crypto War I

- ▶ The 1990s: Wire-tapping vs. cryptography
- ▶ AT&T phone calls encrypted with DH and DES
- ▶ The Clipper-chip and key escrow (broken)
- ▶ Law vs. technology, export control, free speech

Crypto War I

- ▶ The 1990s: Wire-tapping vs. cryptography
- ▶ AT&T phone calls encrypted with DH and DES
- ▶ The Clipper-chip and key escrow (broken)
- ▶ Law vs. technology, export control, free speech
- ▶ EFF DES cracker broke 56 bit DES in 1998

Crypto War I

- ▶ The 1990s: Wire-tapping vs. cryptography
- ▶ AT&T phone calls encrypted with DH and DES
- ▶ The Clipper-chip and key escrow (broken)
- ▶ Law vs. technology, export control, free speech
- ▶ EFF DES cracker broke 56 bit DES in 1998
- ▶ The US government allows crypto from ~ 2000

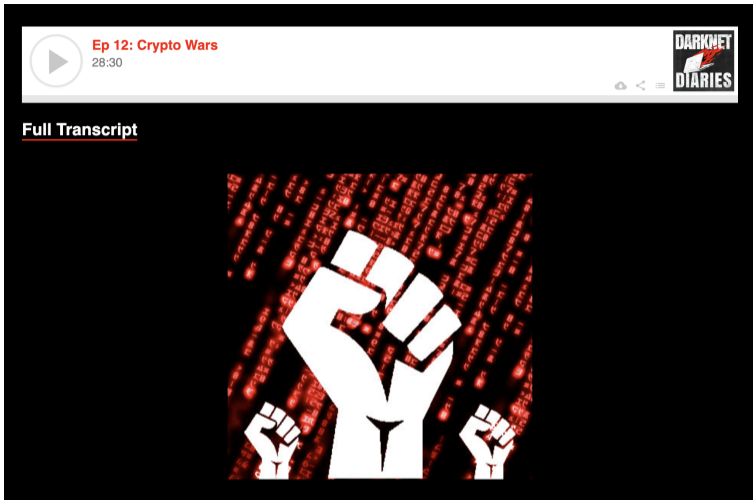


Figure: <https://darknetdiaries.com/episode/12>

Crypto War II

Crypto War II

- ▶ Roughly the years 2010-2016: The "Going dark" debate

Crypto War II

- ▶ Roughly the years 2010-2016: The "Going dark" debate
- ▶ Communication (calls, messages) usually not encrypted

Crypto War II

- ▶ Roughly the years 2010-2016: The "Going dark" debate
- ▶ Communication (calls, messages) usually not encrypted
- ▶ The data stored on phones and laptops was encrypted

Crypto War II

- ▶ Roughly the years 2010-2016: The "Going dark" debate
- ▶ Communication (calls, messages) usually not encrypted
- ▶ The data stored on phones and laptops was encrypted
- ▶ The 2013 Snowden revelations and mass surveillance

Crypto War II


- ▶ Roughly the years 2010-2016: The "Going dark" debate
- ▶ Communication (calls, messages) usually not encrypted
- ▶ The data stored on phones and laptops was encrypted
- ▶ The 2013 Snowden revelations and mass surveillance
- ▶ Crypto vs Mass Surveillance <http://cms16.item.ntnu.no>

Crypto War II

- ▶ Roughly the years 2010-2016: The "Going dark" debate
- ▶ Communication (calls, messages) usually not encrypted
- ▶ The data stored on phones and laptops was encrypted
- ▶ The 2013 Snowden revelations and mass surveillance
- ▶ Crypto vs Mass Surveillance <http://cms16.item.ntnu.no>
- ▶ The FBI vs. Apple case and breaking into devices

Crypto War II

- ▶ Roughly the years 2010-2016: The "Going dark" debate
- ▶ Communication (calls, messages) usually not encrypted
- ▶ The data stored on phones and laptops was encrypted
- ▶ The 2013 Snowden revelations and mass surveillance
- ▶ Crypto vs Mass Surveillance <http://cms16.item.ntnu.no>
- ▶ The FBI vs. Apple case and breaking into devices
- ▶ Standardized crypto backdoored by NSA (next lecture)



Crypto War II: Update from the trenches

Matt Blaze
Sandy Clark
University of Pennsylvania

Figure: <https://youtu.be/bB68G8tLh38>

The Moral Character of Cryptographic Work^{*}

Phillip Rogaway

Department of Computer Science
University of California, Davis, USA
`rogaway@cs.ucdavis.edu`

December 2015
(minor revisions March 2016)

Figure: <https://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf>

Crypto War III

Crypto War III

- ▶ 2017-now: The ongoing "Safety vs. Privacy" debate

Crypto War III

- ▶ 2017-now: The ongoing "Safety vs. Privacy" debate
- ▶ EARN IT ACT, ONLINE SAFETY BILL, CHAT CONTROL 2.0

Crypto War III

- ▶ 2017-now: The ongoing "Safety vs. Privacy" debate
- ▶ EARN IT ACT, ONLINE SAFETY BILL, CHAT CONTROL 2.0
- ▶ Age verification, content scanning, liable providers

Crypto War III

- ▶ 2017-now: The ongoing "Safety vs. Privacy" debate
- ▶ EARN IT ACT, ONLINE SAFETY BILL, CHAT CONTROL 2.0
- ▶ Age verification, content scanning, liable providers
- ▶ Essentially breaks end-to-end encryption in practice

Crypto War III

- ▶ 2017-now: The ongoing "Safety vs. Privacy" debate
- ▶ EARN IT ACT, ONLINE SAFETY BILL, CHAT CONTROL 2.0
- ▶ Age verification, content scanning, liable providers
- ▶ Essentially breaks end-to-end encryption in practice
- ▶ Wants to use AI to discover illegal online content

Crypto War III

- ▶ 2017-now: The ongoing "Safety vs. Privacy" debate
- ▶ EARN IT ACT, ONLINE SAFETY BILL, CHAT CONTROL 2.0
- ▶ Age verification, content scanning, liable providers
- ▶ Essentially breaks end-to-end encryption in practice
- ▶ Wants to use AI to discover illegal online content
- ▶ Swiss Police in 2022: "80 % of reports are false"

Crypto War III

- ▶ 2017-now: The ongoing "Safety vs. Privacy" debate
- ▶ EARN IT ACT, ONLINE SAFETY BILL, CHAT CONTROL 2.0
- ▶ Age verification, content scanning, liable providers
- ▶ Essentially breaks end-to-end encryption in practice
- ▶ Wants to use AI to discover illegal online content
- ▶ Swiss Police in 2022: "80 % of reports are false"
- ▶ No one knows what is target of scanning = backdoor

Keys Under Doormats:

MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL
DATA AND COMMUNICATIONS

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze,
Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann,
Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Figure: <https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf>

PROPOSED AUTOMATIC
SCREENING OF ALL CHATS, EMAILS,
AND MESSENGER CONTENT

[ALREADY IMPLEMENTED BY GOOGLE,
FACEBOOK, AND MICROSOFT]

TEXT AND IMAGE ANALYSIS
WITH ARTIFICIAL INTELLIGENCE

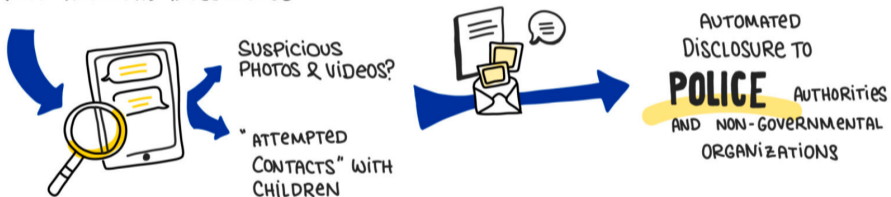


Figure: <https://www.patrick-breyer.de/en/posts/chat-control>

Contents

Announcements

Legacy Crypto

Crypto Wars

An Old Cipher

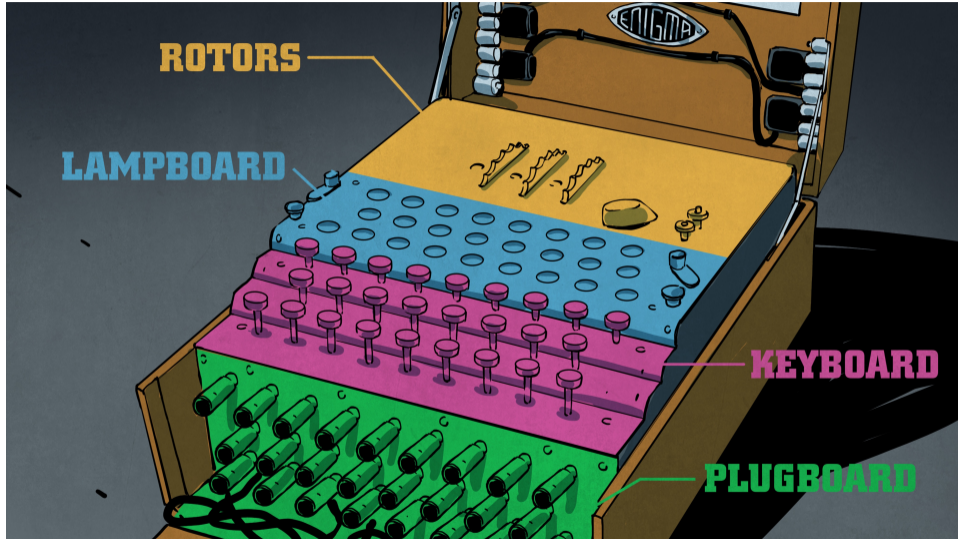
Crypto AG

Newer Ciphers

Newest Ciphers



Enigma Machine



Code Table

Geheim!

Sonder-Maschinenschlüssel BGS

08 *

Nicht ins Flugzeug mitnehmen!

Datum	Walzenlage	Ringstellung	Steckerverbindungen												Kenngruppen			
31.	I II V	10 14 02	BF	SD	AY	HG	OU	QC	WI	RL	XP	ZK	yqv	vuc	xxo	gvf		
30.	V IV I	04 25 01	DI	ZL	RX	UH	QK	PC	VY	GA	SO	EM	mgy	vts	gvt	csx		
29.	III V II	13 11 06	ZM	BQ	TP	YX	FK	AR	WH	SO	NJ	DG	aky	vdv	oyo	tzt		
28.	I III II	09 16 12	NE	MT	RL	OY	HV	IU	GK	FW	PZ	XC	nfh	vce	cqm	wnb		
27.	III II I	06 03 15	BF	GR	SZ	OM	WQ	TY	HE	JU	XN	KD	bec	jmv	vtp	xdb		
26.	I III V	19 26 08	GS	VD	CQ	LE	HI	BO	JP	UZ	FT	RN	wvu	yem	buz	rjk		
25.	II I IV	05 01 16	KA	ZH	QP	GR	MF	LJ	OT	EN	BD	YW	ktv	muq	cqm	cpm		
24.	III II IV	22 02 06	PI	KM	JB	YU	QS	OV	ZA	GW	CH	XF	zcd	iwo	urp	glg		
23.	IV III II	08 11 07	SX	TD	QP	HU	PB	YN	CO	IK	WE	GZ	epm	mgs	vqg	vsm		
22.	I V II	13 02 26	GP	XH	IW	BO	NU	MD	SA	ZK	QR	LT	aam	mvý	jqg	wqm		
21.	IV I V	17 24 03	XC	AQ	OT	UZ	HD	RG	KM	BL	NS	JW	ltl	blu	frk	xrh		
20.	IV I III	15 22 12	PO	TV	QC	ZS	EX	WR	BJ	DK	FU	LA	non	lic	oxr	usr		
19.	V I III	13 24 21	HA	GM	DI	VK	JP	YU	EF	TB	ZL	XQ	ecd	ciq	uvr	ppt		
18.	IV V I	23 09 20	XW	PZ	SQ	GR	AJ	UO	CN	BV	TM	KI	fjh	sts	uqu	cft		
17.	III II V	21 24 15	UT	ZC	YN	BE	PK	JX	RS	GF	IA	QH	oub	eci	pyf	rqi		
16.	IV III V	07 01 13	IN	YJ	SD	UV	GF	BH	TK	QE	AR	OP	kex	paw	flw	onw		
15.	I IV II	15 04 25	TM	IJ	VK	OY	NX	PR	WL	GA	BU	SP	sdr	pbu	byv	knb		
14.	III II IV	10 23 21	WT	RE	PC	FY	JA	VD	OI	HK	NX	ZS	mhz	lff	lnq	gly		
13.	V I II	14 04 12	AN	IV	LH	YP	WM	TR	XU	FO	ZB	ED	rgh	ucm	ldi	ods		
12.	II V I	07 19 02	HR	NC	IU	DM	TW	GV	FB	ZL	EQ	OX	asy	xza	uvc	fmr		
11.	I V IV	13 15 11	NX	EC	RV	GP	SU	DK	IT	FY	BL	AZ	gyd	iuq	ceb	vef		
10.	V II I	09 20 19	VN	TA	YJ	SO	RG	PC	VD	KI	XH	WZ	pyz	ace	pru	úyc		
9.	I IV V	14 10 25	VK	DW	LH	RF	JS	CX	PT	YB	ZG	MU	nyh	fbd	ohs	jrp		
8.	IV V I	22 04 16	PV	XS	ZU	EQ	DW	CH	AO	RL	JN	TD	tck	rts	nro	mk1		
7.	V I IV	18 11 25	TS	IK	AV	QP	HW	FM	DX	NG	CY	UE	mhw	lwb	mdm	ybe		
6.	IV I III	02 17 20	KZ	FI	WY	MP	DS	HR	CJ	XE	QV	NT	uwu	vdk	lrh	mgd		
5.	I V IV	26 09 14	VW	LT	PB	FO	ZK	GS	RI	QJ	HM	XE	suw	tsv	nfp	yjc		
4.	IV III V	07 01 12	QS	YA	XW	KR	MP	HT	DU	OV	CL	FZ	uby	usi	mhh	nwb		
3.	I II V	05 16 03	FW	DL	NX	BV	KM	RZ	HY	IQ	EC	JU	tns	von	grw	axl		
2.	III I II	12 22 17	DW	UO	PY	GR	FS	BQ	KT	CL	AI	ZB	smz	lbl	bkc	sym		
1.	I III II	04 18 06	ZN	OM	CR	UI	KP	WQ	SE	JV	LX	TF	ghr	vqv	cya	ayl		

DECLASSIFIED
 Authority NAD 03/03
 By DP NARA Date 11/4/04

Security of Enigma

Security of Enigma

- ▶ Choose three rotors out of five

Security of Enigma

- ▶ Choose three rotors out of five
- ▶ Each rotor has 26 starting positions

Security of Enigma

- ▶ Choose three rotors out of five
- ▶ Each rotor has 26 starting positions
- ▶ Plugboard connecting ten letter-pairs

Security of Enigma

- ▶ Choose three rotors out of five
- ▶ Each rotor has 26 starting positions
- ▶ Plugboard connecting ten letter-pairs
- ▶ Leads to roughly 2^{67} possible settings

Security of Enigma

- ▶ Choose three rotors out of five
- ▶ Each rotor has 26 starting positions
- ▶ Plugboard connecting ten letter-pairs
- ▶ Leads to roughly 2^{67} possible settings
- ▶ Impossible to break until recent years...

Flaws of Enigma

Flaws of Enigma

- ▶ A plaintext letter can never be encrypted to itself

Flaws of Enigma

- ▶ A plaintext letter can never be encrypted to itself
- ▶ They had access to known plaintexts every day

Flaws of Enigma

- ▶ A plaintext letter can never be encrypted to itself
- ▶ They had access to known plaintexts every day
- ▶ Each contradiction removed millions of settings

Flaws of Enigma

- ▶ A plaintext letter can never be encrypted to itself
- ▶ They had access to known plaintexts every day
- ▶ Each contradiction removed millions of settings
- ▶ It took two hours to brute force a key each day

Flaws of Enigma

- ▶ A plaintext letter can never be encrypted to itself
- ▶ They had access to known plaintexts every day
- ▶ Each contradiction removed millions of settings
- ▶ It took two hours to brute force a key each day
- ▶ Alan Turing and his team broke the code in 1941/42

Facts about Enigma

Facts about Enigma

- ▶ The UK disclosed that they broke it in 1970

Facts about Enigma

- ▶ The UK disclosed that they broke it in 1970
- ▶ There are roughly 300 (publicly known) copies

Facts about Enigma

- ▶ The UK disclosed that they broke it in 1970
- ▶ There are roughly 300 (publicly known) copies
- ▶ Some versions of Enigma have four rotors

Facts about Enigma

- ▶ The UK disclosed that they broke it in 1970
- ▶ There are roughly 300 (publicly known) copies
- ▶ Some versions of Enigma have four rotors
- ▶ The auction value is between 3 and 5 MNOK

Enigma at NTNU



More Enigma

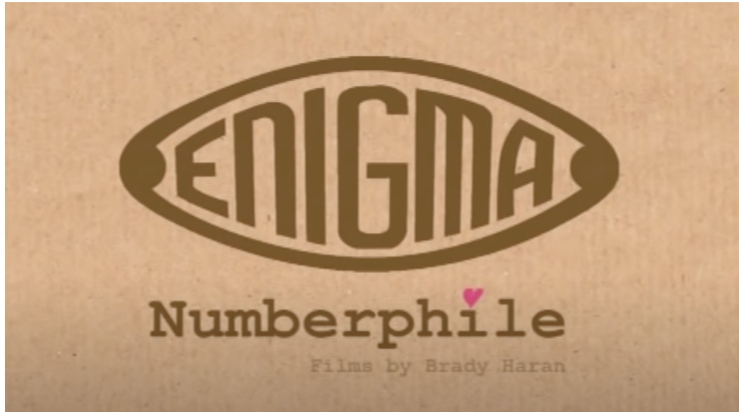


Figure: Numberphile: https://youtu.be/G2_Q9FoD-oQ, and at Computerphile: https://youtube.com/playlist?list=PLzH6n4zXuckodsatCTEuxaygCHizMS0_I

Contents

Announcements

Legacy Crypto

Crypto Wars

An Old Cipher

Crypto AG

Newer Ciphers

Newest Ciphers

A Swiss company named Crypto AG, funded by the Swede named Boris Hagelin, sold encryption machines to nation states all over the world after the second world war. They were similar to the Enigma machine.

Widespread Usage

THE AMERICAS

Argentina
Brazil
Chile
Colombia
Honduras
Mexico
Nicaragua
Peru
Uruguay
Venezuela

EUROPE

Austria
Czechoslovakia
Greece
Hungary
Ireland
Italy
Portugal
Romania
Spain
Turkey
Vatican City
Yugoslavia

AFRICA

Algeria
Angola
Egypt
Gabon
Ghana
Guinea
Ivory Coast
Libya
Mauritius
Morocco
Nigeria
Rep. of the Congo
South Africa
Sudan
Tanzania
Tunisia
Zaire
Zimbabwe

MIDDLE EAST

Iran
Iraq
Jordan
Kuwait
Lebanon
Oman
Qatar
Saudi Arabia
Syria
U.A.E.

REST OF ASIA

Bangladesh
Burma
India
Indonesia
Japan
Malaysia
Pakistan
Philippines
South Korea
Thailand
Vietnam

WORLDWIDE ORGANIZATION

United Nations

The records show that at least four countries — Israel, Sweden, Switzerland and the United Kingdom — were aware of the operation or were provided intelligence from it by the United States or West Germany.

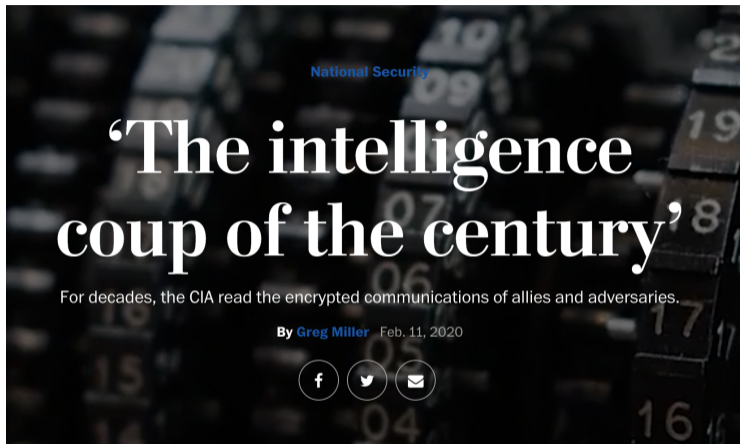


Figure: <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage>

Contents

Announcements

Legacy Crypto

Crypto Wars

An Old Cipher

Crypto AG

Newer Ciphers

Newest Ciphers

Legacy Ciphers

Several newer ciphers developed in the 1990s and 2000s were the leading standards for many years, and they are still used in various protocols and products used on or connected to the Internet today.

There has been a variety of attacks, and here are some examples...

MD5

- ▶ Hash function outputting 128 bits
- ▶ Designed by Ron Rivest in 1991
- ▶ First specific collisions found in 2004
- ▶ First general collisions found in 2006
- ▶ Used to create fake X509 certificates
- ▶ Revoked in most (!) applications by 2014 (!)

Year	Identical-prefix collision cost	Chosen-prefix collision cost
< 2004	2^{64} generic	2^{64} generic
2004	2^{40} [WY05]	—
2005	2^{37} [Kli05]	—
2006	2^{32} [Kli06, Ste06]	2^{49} [SLdW07c]
2007	2^{25} [Ste07]	—
2008	2^{21} [XLF08]	—
2009	2^{16} [SSA ⁺ 09]	2^{39} [SSA ⁺ 09]
2020	2^{16} [SSA ⁺ 09]	2^{39} [SSA ⁺ 09]

Figure: <https://www.marc-stevens.nl/research/papers/CC21Chapter-S.pdf>

RADIUS/UDP vulnerable to improved MD5 collision attack

2024-07-09



Sharon Goldberg



Miro Haller (Guest Author)



Nadia Heninger (Guest Author)



Michael Milano (Guest Author)



Dan Shumow (Guest Author)



Marc Stevens (Guest Author)



Adam Suhl (Guest Author)

Figure: <https://blog.cloudflare.com/radius-udp-vulnerable-md5-attack>

RADIUS/UDP Considered Harmful

Sharon Goldberg
Cloudflare

Miro Haller
UC San Diego

Nadia Heninger
UC San Diego

Mike Milano
BastionZero

Dan Shumow
Microsoft Research

Marc Stevens
Centrum Wiskunde & Informatica

Adam Suhl
UC San Diego

Figure: <https://www.blastradius.fail/pdf/radius.pdf>

SHA-1

- ▶ Hash function outputting 160 bits
- ▶ Designed by the NSA in 1995
- ▶ First specific collisions found in 2017
- ▶ First general collisions found in 2020
- ▶ Revoked in most (!) applications by 2020 (!)

SHA-1

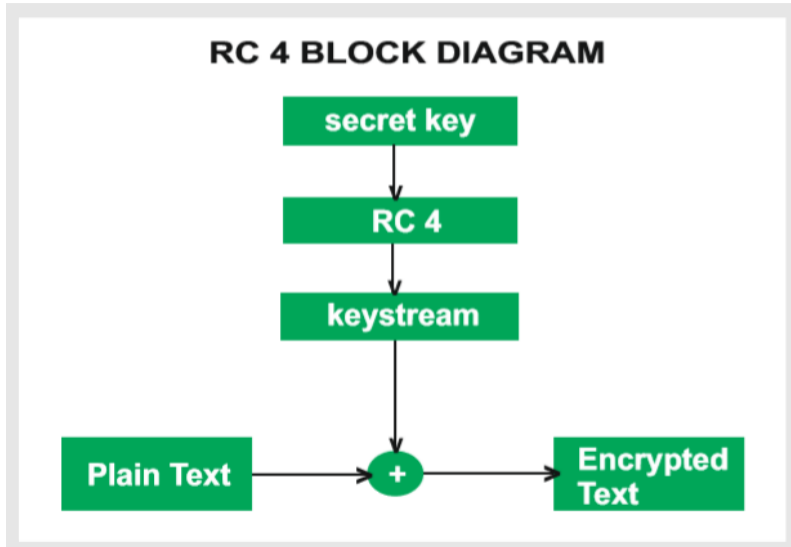
Year	Identical-prefix collision cost		Chosen-prefix collision cost	
< 2005	2^{80}	generic	2^{80}	generic
2005	2^{69}	[WYY05b]	–	
	($u : 2^{63}$	[WYY05a])	–	
2007	($u : 2^{61}$	[MRR07])	–	
2009	($w : 2^{52}$	[MHP09])	–	
2013	2^{61}	[Ste13b]	2^{77}	[Ste13b]
2017	G : $2^{63.1}$	[SBK ⁺ 17]	–	
2019	–		$G : 2^{67}$	[LP19]
2020	$2^{61} / G : 2^{61.2}$	[Ste13b] / [LP20]	G : $2^{63.4}$	[LP20]

Figure: <https://www.marc-stevens.nl/research/papers/CC21Chapter-S.pdf>

RC4

- ▶ Symmetric stream cipher using at least 40 bit keys
- ▶ Designed by Ron Rivest in 1987 (public in 1994)
- ▶ Used in the WEP (1997), WPA (2003), SSL/TLS (1995)
- ▶ Detectable bias after only 256 bytes of data
- ▶ Long list of attacks. Broken in WEP in 2004.
- ▶ Revoked in most (!) applications by 2015 (!)

RC4



Weaknesses in the Key Scheduling Algorithm of RC4

Scott Fluhrer¹, Itsik Mantin², and Adi Shamir²

¹ Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134
sfluhrer@cisco.com

² Computer Science department, The Weizmann Institute, Rehovot 76100, Israel.
{itsik,shamir}@wisdom.weizmann.ac.il

Figure: https://www.mattblaze.org/papers/others/rc4_ksaproc.pdf

3DES

- ▶ DES: Symmetric block cipher using 56 bit keys
- ▶ Proposed in 1981, standardized in 1995 by NIST
- ▶ 3DES: Using DES three times with three keys
- ▶ Meet-in-the-Middle attack: 112 bits of security
- ▶ Revoked in most applications by 2019

Contents

Announcements

Legacy Crypto

Crypto Wars

An Old Cipher

Crypto AG

Newer Ciphers

Newest Ciphers

ARADI and LLAMA: Low-Latency Cryptography for Memory Encryption

Patricia Greene
Mark Motley
Bryan Weeks

National Security Agency
9800 Savage Road, Fort Meade, MD 20755, USA

{ppgreen, mjmotle}@nsa.gov, bewecks@uwe.nsa.gov

Abstract

In this paper, we describe a low-latency block cipher (ARADI) and authenticated encryption mode (LLAMA) intended to support memory encryption applications.

Figure: <https://eprint.iacr.org/2024/1240.pdf>



A Note on ARADI and LLAMA

Roberto Avanzi^{1,2}, Orr Dunkelman³ and Shibam Ghosh³

¹ Qualcomm Germany GmbH, Munich, Germany

ravanzi@qti.qualcomm.com

² Caesarea Rothschild Institute, University of Haifa, Haifa, Israel

roberto.avanzi@gmail.com

³ Computer Science Department, University of Haifa, Haifa, Israel

orrd@cs.haifa.ac.il, sghosh03@campus.haifa.ac.il

Abstract. Recently, the NSA has proposed a block cipher called **ARADI** and a mode of operation called **LLAMA** for memory encryption applications. In this note, we comment on this proposal, on its suitability for the intended application, and describe an attack on **LLAMA** that breaks confidentiality of ciphertext and allows a straightforward forgery attack breaking integrity of ciphertext (*INT-CTXT*) using a related-*Initialization Vector* (IV) attack. Both attacks have negligible complexity.

Figure: <https://eprint.iacr.org/2024/1328.pdf>

Questions?