NTNU | Norwegian University of Science and Technology

LEGACY CRYPTO 1

TTM4205 – Lecture 5

Tjerand Silde

05.09.2023

Contents

Contents

Uniped Observation

I am completing a course in University Pedagogy (Uniped) this year, and today, I have so-called *collegial coaching*. This means that a few other lecturers from different departments at NTNU will observe my lecture and provide feedback afterward. They are **not** observing you.

Reference Group

I am looking for (at least) three students to form a reference group in this course, preferably students from different programs. We will meet three times during the semester, and your feedback is extremely valuable.

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

Open PhD Position

Figure: https://www.jobbnorge.no/en/available-jobs/job/246480/phd-candidate-in-cryptography-engineering

Contents

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- Old and outdated crypto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- Old and outdated crypto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- Old and outdated crypto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- Old and outdated crypto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

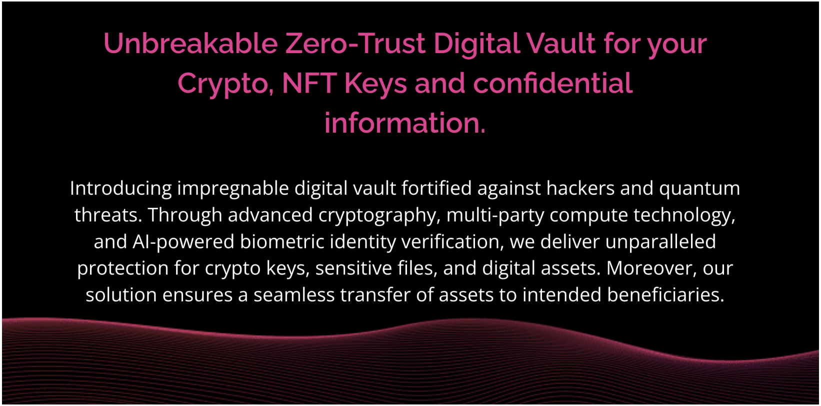
Legacy Crypto is...

- Old and outdated crypto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- Old and outdated crypto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

Legacy Crypto $\neq$ Crypto Legacy



Two Categories

Secret Key Crypto

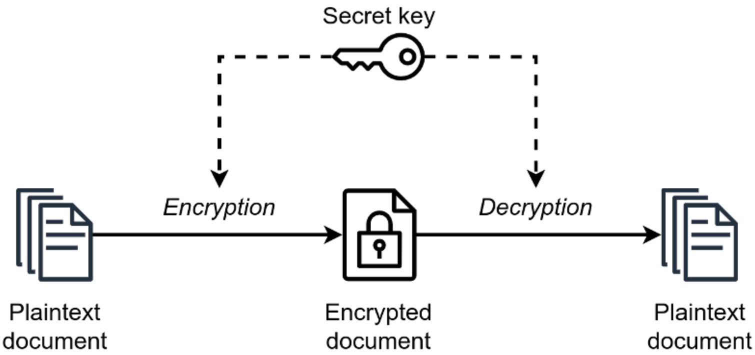
Public Key Crypto

Today

Secret Key Crypto

Public Key Crypto

Secret Key Crypto



Contents

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

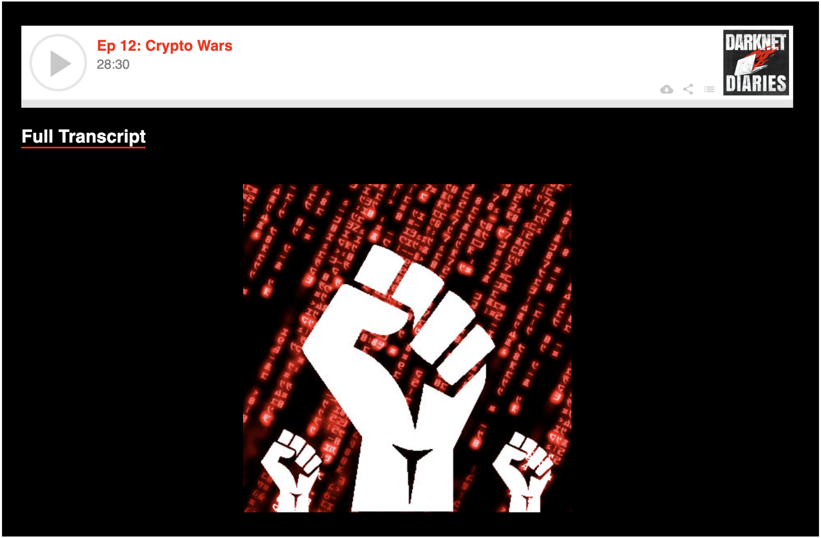


Figure: https://darknetdiaries.com/episode/12

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 stored data 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 stored data 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 stored data 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 stored data 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 stored data 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)

Figure: https://youtu.be/bB68G8tLh38

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:

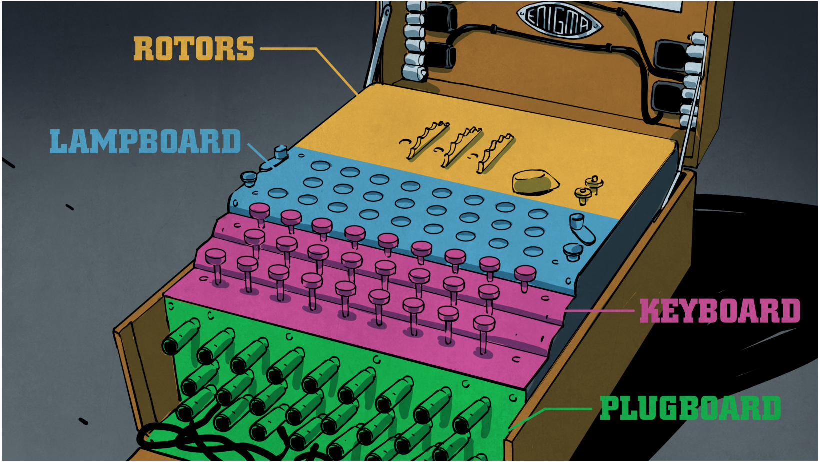
MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS

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://spar.isi.jhu.edu/~mgreen/paper-keys-under-doormats.pdf`

Contents

Enigma Machine



Code Table

Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

08 ❊

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	mqy	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	vco	tur	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	FB	YN	CO	IK	WE	GZ	epm	mgz	vqg	vsm
22.	I	V	II	13	02	26	GP	XH	IW	BO	NU	MD	SA	ZK	QR	LT	aam	mvy	jqq	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	XF	PZ	SQ	GR	AJ	UO	CN	BV	TM	KI	fjh	zts	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	SF	sdr	pbu	byv	khb
14.	III	II	IV	10	23	21	WT	RE	PC	FY	JA	VD	OI	HK	NX	ZS	mhz	lff	lnq	giy
13.	V	I	II	14	04	12	AN	IV	LH	YP	WM	TR	XU	FO	ZB	ED	rqh	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	ocb	vef
10.	V	II	I	09	20	19	FN	TA	YJ	SO	EG	PC	VD	KI	XH	WZ	pyz	ace	pru	uyc
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	BW	CH	AO	RL	JN	TD	tck	rts	nro	mkl
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	CU	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	mwb
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	EQ	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

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

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

Legacy Ciphers

We have several newer ciphers developed in the 1990s and early 2000s that were the leading standard for many years, and we still find them in a variety of protocols and products that are still used on or connected to the Internet today.

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

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 (!)

MD5

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

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	$\mathbf{G : 2^{63.1}}$	**[SBK+17]**	–	
2019	–		$G : 2^{67}$	[LP19]
2020	2^{61} / $G : 2^{61.2}$	[Ste13b] / [LP20]	$\mathbf{G : 2^{63.4}}$	**[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 (!)

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

AES-CBC

AES-CBC

- Cipher mode for symmetric ciphers (e.g. AES)

AES-CBC

- Cipher mode for symmetric ciphers (e.g. AES)
- Proposed in 1976, proven in 1997, broken 2002

AES-CBC

- Cipher mode for symmetric ciphers (e.g. AES)
- Proposed in 1976, proven in 1997, broken 2002
- CPA secure (theory), not CCA (practice), patched

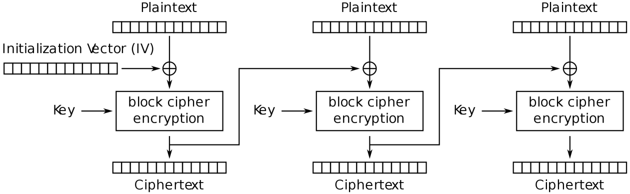
AES-CBC

- Cipher mode for symmetric ciphers (e.g. AES)
- Proposed in 1976, proven in 1997, broken 2002
- CPA secure (theory), not CCA (practice), patched
- A variety of padding oracle attacks in practice

AES-CBC

- Cipher mode for symmetric ciphers (e.g. AES)
- Proposed in 1976, proven in 1997, broken 2002
- CPA secure (theory), not CCA (practice), patched
- A variety of padding oracle attacks in practice
- Revoked from some applications (e.g. TLS) in 2018

AES-CBC



Cipher Block Chaining (CBC) mode encryption

CBC Attack

CBC Attack

- Each block must be of exactly 128 bits

CBC Attack

- Each block must be of exactly 128 bits
- Shorter message leads to padding at the end

CBC Attack

- Each block must be of exactly 128 bits
- Shorter message leads to padding at the end
- Add one byte ends with 01, two with 02, etc. ...

CBC Attack

- Each block must be of exactly 128 bits
- Shorter message leads to padding at the end
- Add one byte ends with 01, two with 02, etc. ...
- An API outputs errors when wrong padding

CBC Attack

- Each block must be of exactly 128 bits
- Shorter message leads to padding at the end
- Add one byte ends with 01, two with 02, etc. ...
- An API outputs errors when wrong padding
- The error message or timing might leak info...

CBC Attack

CBC Attack

- Let C_2 be an encryption of X that you want to decrypt

CBC Attack

- Let C_2 be an encryption of X that you want to decrypt
- Choose random C_1 and ask for $C_1|C_2$ to be decrypted

CBC Attack

- Let C_2 be an encryption of X that you want to decrypt
- Choose random C_1 and ask for $C_1|C_2$ to be decrypted
- Successful decryption if $C_1 \oplus X$ has valid padding

CBC Attack

- Let C_2 be an encryption of X that you want to decrypt
- Choose random C_1 and ask for $C_1|C_2$ to be decrypted
- Successful decryption if $C_1 \oplus X$ has valid padding
- Vary last byte of C_1 until correct to find last byte of X

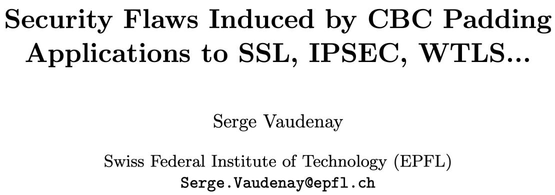
CBC Attack

- Let C_2 be an encryption of X that you want to decrypt
- Choose random C_1 and ask for $C_1|C_2$ to be decrypted
- Successful decryption if $C_1 \oplus X$ has valid padding
- Vary last byte of C_1 until correct to find last byte of X
- Find next byte by $C_1[15] = X[15] \oplus 02$ and vary $C_1[14]$

CBC Attack

- Let C_2 be an encryption of X that you want to decrypt
- Choose random C_1 and ask for $C_1|C_2$ to be decrypted
- Successful decryption if $C_1 \oplus X$ has valid padding
- Vary last byte of C_1 until correct to find last byte of X
- Find next byte by $C_1[15] = X[15] \oplus 02$ and vary $C_1[14]$
- Continue until you have all bytes of X, max $128 \cdot 16$ trials

CBC Attack



Security Flaws Induced by CBC Padding
Applications to SSL, IPSEC, WTLS...

Serge Vaudenay

Swiss Federal Institute of Technology (EPFL)
Serge.Vaudenay@epfl.ch

Figure: https://www.iacr.org/cryptodb/archive/2002/EUROCRYPT/2850/2850.pdf

Questions?