

Cryptography

Secure Software Systems

Will try to stay above the math as much as possible...

State (Dr dNi=

20

1125(2),

dNT=

(TTL)

(Xnt= D)

Vz

Useful References on Class Website

Cryptography

- Crypto 101 e-book [Free/PDF, (2017+)]
 - Written by Laurens Van Houtven and distributed at https://www.crypto101.io/. Updated directly at GitHub repo. (See also: Local mirror, may be out of date compared to github copy)
 - Big picture ideas + Commentary on breaking crypto. Light on the math! Incomplete / work in progress.
- Cryptography: An Introduction (3rd Edition) [Free/PDF, 2006]
 - Written by Nigel Smart, a cryptographer & computer science professor specializing in the area of elliptic curve cryptography.
 - Note: The free e-book is no longer being updated as-of 2016. See Cryptography Made Simple (2016, Springer Publishing) for purchase.
 - Heavy on the math!
- Cryptography Engineering [Paid, 2010]
 - Written by Niels Ferguson (Cryptographer, Microsoft), Bruce Schneier (Cryptographer), and Tadayoshi Kohno (Professor, University of Washington)



+**CRYPTO**101

Crypto 101 is an introductory course on cryptography, freely available for programmers of all ages and skill levels.

Get current version (PDF)

7 5 У Tweet

Start to finish.

Comes with everything you need to understand complete systems such as SSL/TLS: block ciphers, stream ciphers, hash functions, message authentication codes, public key encryption, key agreement protocols, and signature algorithms.

Learn by doing.

Learn how to exploit common cryptographic flaws, armed with nothing but a little time and your favorite programming language.

Forge administrator cookies, recover passwords, and even backdoor your own random number generator.

https://www.crypto101.io/

Has a video too!

https://www.youtube.com/watch?v=3rmCGsCYJF8

Works everywhere.

DRM-free and available in all common formats:

- PDF (for Mac and PC)
- EPUB (for most ebook readers, iPad and iPhone)
- Mobi (for Kindle)

XOR & One Time Pads



6



Useful XOR Properties

- Associative: Apply XOR in any order: $a \bigoplus (b \bigoplus c) = (a \bigoplus b) \bigoplus c$
- Commutative: Flip operands around: $a \bigoplus b = b \bigoplus a$
- ✓ Useful property for encryption:
 a ⊕ b ⊕ a = a ⊕ a ⊕ b
 = 0 ⊕ b
 = b

7

One-Time Pad (OTP)

ADDRESSON	AGERE AGERE AGERE RELLTE AGGERE LZEJRT	13242	CHESTATINE THREE49	MALMOSLG	and the states of		and a second second	
ALLEARNELL DELLARREL DELECARREL DELECARREL <th>ONDER CINDEN RELLIE ABGNEG LERBE</th> <th></th> <th>THEFELS</th> <th>and the second second second</th> <th></th> <th>49 7 18 HB CA MM 28 87</th> <th>AN</th> <th>and the second second second second</th>	ONDER CINDEN RELLIE ABGNEG LERBE		THEFELS	and the second second second		49 7 18 HB CA MM 28 87	AN	and the second second second second
AFFERENCIES CONTROLLER STRUCTURE CONTROLLER CONTROLLER CONTROLLER CONTROLLER STRUCTURE CONTROLLER CONTROL CON	CYRDEN RELLTE ABGERG LERBRT			SHITTWAGE	PBXWYTXR	PDLLPH92	ORRENOW	RNRZLOYX
PARCHBAR PSRBNPRN EXHQUNNE ALSCY74B PARCABAR GDCL2346 ALS SHARMSGRY WBKHLJERE SQYNCD YT RQ7XQ6WE PCTQBGGY D78EL6E7 BE 4326643W SYAEHQQ9 DEHE67NB GSWN6C7M NBGR26EF 72223GF2 LG 7. EM6MCGEN BEXNERRAY SKLMANSC C4DHN83H KSLNQC7F SER3MES 9 N27P7ERG T2MEAGY LG4663M7 XSLMANSC 7000000000000000000000000000000000000	ABGXR6 L2X3RT		DERABSS	RYABCQ48	GENESSEN ACTESVIE	RDL29522	THTRIZME	NY JZBLQJ ADB 33702
SHXWMGRY WSXMLSRE SQYNCDY* NQYXGAWE PC7QBGGY DYNLGET DE 43Q6643W SYXAEHQQ9 DENEG7RS G3WS6C7N NEGR26EF 72223GF2 L 7. LM6MCGZH EDXNRRA? SXLDAMSGC C4DHENSH E52MQC7F 62EB3XZES 9 M22Fr4f HI3AD329 RSFR3EXX F9SXA6326 7R88FS865 SYZPERRH XX GTESTOPM L64663N7 XXLNSAST F9SXA6325 7R88FS865 SYZPERRH XX GTESTOPM L64663N7 XXLNSAST F9SXA6325 7R88FS865 SYZPERRH XX GTESTOPM HERTER26 SGYZLHWM BNTYSCF3 XXSMPF70 SQMQFXY F7 NLLF3AXE SYAASHER H2X4LE29 PNF3732F RQXNTCF3 XXRNKGRC7F F7 GCAASKENCH SYZZASHY H27BC4728 SQMYCG77 ZESACT F8X7333C2 SZ SZ 90434KXX Q4CREAK NYZZENY7 H7 H78C728 FGCMMRQ7 ZF94CTRR M2 8. AAR5 T77EC728 SZMYCAT ZYXTD826 PRE PRE	LIXIBT		GPCD2446	F4XNAND4	41.900748	RENORNER	PORSEPHEN	PAEC43AK
4326643W DYAEHQQ9 DEHE6789 G3M86C7M NEGR26EF 72223GF2 11 7. 1.66MCGZH EDXNERAY 2.NLB4BBG C4DHB89H E6520007F 62B3X2E3 9 M22KP4T HT3AD329 RSFR3BXX F952A4325 7RB3FB26 SY2F2RRH X W77F787C T2WB2GYW L64663H7 X72.R5877 FW2YXCF3 XARNH6HG 77 GTEN7OFM 4PBITR26 SCF2LMWM BNY76CFA Y36MP70 ECM4QFXY F7 NLLP3AX2 BYAASHFK H324LE25 BOF3139W L4326MTC 76LY373C2 52 96334K8X2 Q4CBR6KK M222BTY7 9XD6WTX5 B4E283L4 SCHCON77 WC C2A2MW2B D6FF 77X56WLFE 22LTY773 FT0CMMRC7 2F94CTRR 4W M37MMQ37 P' 'G224BW 012H4377 2967668X NDRXYLXE 2G 8. 6. 6. 6. 6. 6. 6. 6. 6. 6. 6			D78EL6E7	FC7QBGGY	ROTXOGNE	2QYNCD77	WEXNLERE	ZHXMMGRY
7. Imbériger Nerser Streiner	A7CNL9		72023692	NBGR26EF	GINASC7N	DZHE67R9	oyabhqqq	4325643%
7. MAGNOGZH BOXNERRAY SXLMANEG CADHENSH KALWOCT SXLPARE SXLPS POLY DN22KPAT HIJADJZS KILMANEG CADHENSH KALWOCTS KARNERS T SYPTATC TEMBOGY LGAGASAN KILAANEG CADHENSH KALWOCTS KARNERS T SYPTATC TEMBOGY LGAGASAN KILAANEG CADHENSH KALWOCTS KARNERSS T SYPTATC TEMBOGY LGAGASAN BNT76CPA YJENYYCH SKLPARESS T SULPJAKE SYAASBERK HIXALESS RMF3728F KQLNTLAS TEMBYYCH T SG334KXX CACHERSK BYZJENY B SC3N339M LAJZANTC TELYJACS DF GARNENCH HINGLO HINGLESS RMF3728F SQLNTC TELYJACS DF GARNENCH HINGLO HINGLESS RMF3728F SC2LTYFTS FIGHNEGT TEL SG334KXX CACHERSK BYZJENY B SC3N339M LAJZANTC TELYJACS DF GCAR SYNNOBT D' GZ24BW DLZHARY Z96TGENSK NDRKYLXE 2G 8. SKBAR TYNNOBT D' GZ24BW DLZHARY Z96TGENSK NDRKYLXE 2G SKAR SYNNAS HINGLESS TYNE HINGLESS M22 SKBAR THASSE SKIFT B SC3NYFT SKRAFT TYNS SKNEWYCH T SKBAR THASSE SKIFT SKRAFT SKRAFT SKRAFT TYNS SKNEWYCH T SKBAR THASSE SKIFT SKRAFT SKRAFT SKRAFT SKRAFT TYNS SKNEWYCH T SKBAR THASSE SKRAFT SKRA								
LMSMCGZE EXXMPRAY SXLMANEG C4DMINSSH KSLNCYTF SZRXENS 9 DN22XP47 HTBAD329 RSFR3BXA P9XA4325 TRBSP326 SYZPREH XX M27P7EXEC T2ME2GYM L6466SN7 XXX.RSRYT FN9YXCF3 XANNHSEN YX GTTS70FM 4PRTFR26 SGP2LNMM BNT76CFA Y3MPP70 EQNACFAN YX NLLP3AXE SYASSNER H2X41E29 BNF3725F RQXNFL69 TBMMNGFC YX CH3NKNOM SYAASANE H2X41E29 BNF3725F RQXNFL69 TBMNNGFC YX CH3NKNOM SYAASANE H2X41E29 BNF3725F RQXNFL69 TBMNNGFC YX CABKKNOM SYAASANE H2X41E29 BNF3725F RQXNFL69 TBMNNGFC YX GG834SX2 G4CERACK SWERTY F SYAASANE GWKRNC77 WC AX G2248W OL2M4A27 Z9676CHA L74H6H34 M22 SYAMPOB7 FX SYAAFA GWKRLLRD SYAAFASC M22 SYAAFASC MAX65 T756CF22 SZMYYCH7 SYAAFASC								7.
LMAMEGER BEXNERAT SKIRABSG CADREAS FOR SAVE FOR SKRINGS SYSTEMS DN22NP4T HIJAD325 RSFR3BXA P9SA4355 TRBSPB26 SYSTEMS M27P7RIAS T24RE2GYN L64663N7 KYSLRASRY PNGYXCFT3 XANNAK6853 T GITH7QFM 4PRTFR26 SGP2LNNM BN176CPA Y33MPP70 EQN4QFXN FT NLLP3AXE BYASSNEN N2X4LE35 BNP3755F NOLNFL69 THMMWGPC FT CHARRNOM E3RC42C6 46W9R746 SCHMAS9M L4325MTC 76L3Y33C2 SN SG93483X C44CR66KN N2X4LE25 BNP3755F NOLNFL69 THMMWGPC FT C2A2MW2B D6FP TXE6WLPE 22L1TYTS FJCMRHC7 ZF9ATTER 4W M3YMRQBT F' 'G2248W DL2M4AY7 296T6CHX NDRXYLXE 2G 8.								
BRZZEWAT HIBADBER REFERENCE PESCHARE FACEPACE SYZPERE X M27F7ETC T2WHEGYW L64663N? XYLRESTY FHQYXCF3 XARNHERS T GTTETOTM HERTER26 SERIENN BNT76CPA Y3SMPP70 EQMACRYY F NLLP3AXE BYASSNER N2X4LE29 PMFBTZ9F RQLNFL69 THMMWERC F GGBRENOM EBRC42CE 45N98748 SCB3M39M L4326WTC 76LY93C2 22 9G934K3X Q4CER6KK NE22BTY7 97D6WTXL 84E288LH GWRCNCYT HC C2A2MW2B DEFF TXSCWLFZ 22LYFTS FGCMRMC7 2F94CTRR 44 M3XMRQB7 F 77 G2248W D12R4437 296T6CHX NDRXYLNE 2G 8. 8. 8. 8. 8. 8. 8. 8. 8. 8.	ICA49X8		SZR3XZE3	RETACCIA	CEDEBESS	INDB483G	BOXINERA?	LM6MCGZH
M2797EXE T2WERGYW L64863M7 KYLRESTY FHQYXCF3 XARRHERE T GTENQTM 4PBTER26 GCERLENN BNY76CFA Y32MPF7Q EQNACTAY FY NLLP3AXE BYAASNER H2X4LE29 BNY372.9F RQLKFL69 7HMNWGFC FY CHRRENQM E3RC42CE 4EWBY748 SC334339M L4326MPC 7ELY595C2 E3 9G334K3X C4CHR6KK ME22BTY7 9YD6W3KE R4E2B3LM GWKGNC77 RC C2AZMW2B D6FF TEXEWLFE 2ELYFF93 FGCMMNQ7 2F94CTRR 4W MSYMRQB7 FY G224BW DL2R4&27 296T6CHX NDEXYLKE 2G 9. 9. 9. 9. 9. 9. 9. 9. 9. 9. 9. 9. 9.	SEFL23	[SY2P2RRH	7Respeze	Pysaaszg	R9FR3BXA	HTBAD329	DNIZKPAT
GTTEFJQFN 4FBTFR26 SGF2LSNN BNT76CFA Y3KNPP7Q SQN4QFXY FT NLLPJAXI BYA69MFK HIX4LEIS BNR31Z3F KQINFL65 7HMCNGFC FI CH8KKNQN E3RC42CE 4FM9E788 SC53N339M L4326MTC 78LY93G2 22 SG934KSX G4CER6KN HIZ2ENTY STK4W1X5 B4ES85LM GWKCRC77 MC C2azMW2B D6FP TKE6WLPE 2ELTYFTG FGCMRNQ7 2F94CTRR 4W MFXMRQB7 F' 'G2248W DL2N44X77 296T6CHX NDRXYLXE 2G 8. S2 AAR6 7T7EC22E 92MYYCH7 2Y1TB82C PRE 8CWA 9XHKFWIK GWERLLED 9FXE6F3R PRE 8CWA 9XHKFWIK GWERLED 9FXE6F3R PRE 8CWA 9XHKFWIK GWERLED 9FXE6F3R PRE 8CWA 9XHKFWIK GWERLED 9FXE6F3R PRE 8CWA 9XHKFWIK GWERLED 9FXE6F3R PRE 8CWA 9XHKFWIK 9X 9KG270F 7F4590	TROTOTT	:	XARBHGHG	FROXXCF3	XILR62II	L64863N7	TZWEZGYW	¥27¥7¥%
NLLPJAXE BYAKSNER HEXALESS PMP372.9F RQLNFL&9 TENMARGEC F: CHRRENQN E3RC42CE 45W3R748 9C33M339M L432SMFC 7ELY93C2 32 9693A5X3X C4CBR6KK ME22BYY 9TR6W73K5 84E283LM GWKGNC7F MC C2R2MW2B D6FP TIZEGWLPE 2ELTYPES FGCWMSD7 2F94CFR 4W MSYMRQB7 P "G224BW DL2R4&77 296T6CHX NDRXYLKE 2G 9. 9. 6. 6. 6. 6. 6. 6. 6. 6. 6. 6. 6. 6. 6.	APKZXX		EQM4QFX8	Y33MPP7Q	BNT76CPA	SCPELENN	APBTER26	GTTH7QFX
CHARKENCH E3RC42CE SEW9E74B SCS3M39M L4326MTC 782Y93G2 20 9G936K3X Q4CERACK ME22RTY7 9TR6WTX5, 84E286LH GMKGNC77 MC C2AZMW2B D6FP TXE6WLPE 225JYPT3 FGCMRHQ7 2F94CTRR 4W MFYMRQB7 P "G224BW DL2N44T7 296T6CHX NDRXYLXE 2G 9. 9. 9. 9. 9. 9. 9. 9. 9. 9. 9. 9. 9.	KENDXZ.		TEMMWGEC	ROLNFLSS	PMF3TZ9F	NEX4LEES	BYASSNER	MLLPBAXE
363348XX C4CERR6KE NE22BTY7 STR6WTXL R4E2SSLM STRKENCTT NCCERNENCT NCCERNENCT NCCERNENCT NCCERNENCT STRKENCTT STRKENCT STRKENCTT	BCEXCO		781.99302	1.4326MTC	9C.93N39M	48498748	E3RC42CE	CHARKNON
C2AZMW2B DEFPT TXXEGWLPE 2221973 FGCMMMQ7 2F94CTRR 4W MFXMRQB7 PT TXXEGWLPE 2224BW BL2W4XT7 296T6CHX NDRXYLXE 2G 9. 57 8. 58 8. 59 8. 59 8. 59 8. 50 7. 50 8. 50 8. 50 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	YREEMY		GWRGNC77	24E288LH	9YD6WIXI	NE22BTY7	Q4CBR6KK	9G934X3X
ABYMRQB7 P° "GZ248W DL2R4& 7 296T6CHX NDRXYLXE 2G 9. 53 8 ARE 777ECF2E 92NTYCH7 2Y1.TD82C PR ARE 777ECF2E 92NTYCH7 2Y1.TD82C PR 8 ARE 777ECF2E 92NTYCH7 2Y1.TD82C PR 8 CKA 5X2KTWLK GWERLLED 9FXEF52E PR 8 DTK7 EDALXYWS BANNSP6 MYLN38RP XW9 5 R9A2 704KG123H BUY23Q4T NFG37NF8 NOCH 44EYXE DQFYGBBG M9726DXE EWACP82Q 72KE 722CKD E2CQC226 4K5Y2TPT NEHYTCKC Q2CK 722CKD E2CQC226 4K5Y2TPT NEHYTCKC Q2CK 766AX9C XHEDENGH LK97QYFD TFN5YDGB G2K6 766AX9C XHEDENGH LK97QYFD TFN5YDGF G2K6 7677K5 BUYCKF BY	SSTNNX		2F94CTRE	FGCMREOT	22LTYPTG	TREGULPE	DEFPT	CZAZMWZB
8. S2 N AARS 7TYSCR22 92NYYCH7 2YLTD82C PAR AARS 7TYSCR22 92NYYCH7 2YLTD82C PAR GCWA BX2KTWAR GWERLLRD 9FXE6F3R PMX BELAXTWA BAANN96 MYLN38RP XW SKBAA THARCLEN DFNN92F2 WBYYKCHF LSB KBK9K FX96KFNF NYY23Q4T NFC97NE3 NDC1 X4EYXE DQFYGBBG M8726DXB EMACP82Q 72M2 T22CKD E2CQCR26 4B6Y2TPT N6HYTCKC Q2CH 7M6AK9C XHEDBNGH LK87QFFD T6M5YDGB G2K6 7M6AK9C XHEDBNGH LK87QFFD T6M5YDGB G2K6 7M6AK9C XHEDBNGH KA7QFFD T6M5YDGB G2K6	CANED		NDEXYLXE	2967608X	01.284487	~G2248W	pr	HFYMRQ87
ZBCKEJGN NGYDSNJG SYZCSEQC RENR488X STJC TSAEW3MT 4YYNTYN3 R22ZM4JH AZC323FP HE4Q CHEMY3PA ENCREREN DCHR83TB 6QCYYJR5 DAEQ CHEMY3PA ENCREREN DCHR83TB BAYJCKE SPERT	ZEAFM XK PRD AESE2 DEEN IGLCA RXLC R7TX FCYG RMYK	M P1 K9 L6 MD 72 Q2 G2	LT486834 271.TD820 9FXE6F38 MY1R38RP WBWYNCNF MEG97NE3 EWACP820 NGWYTCKC TFN6YDGE	CLEFND 40 92NTYCH7 GWERLLRD BAJNN9P6 DFNM9RFB RIY23QWT M8T26DXE 4R6Y2TFT LK67QYFD	N2887mgw 7T78CR28 8x287w28 RDALXYN8 7N480L9N 989687NF DQF7688G 82020286 XHED6NGB	46ER DARS BCWA IDTM7 KRBAA KBK9K I4EYXR 722CKD IM6AK9C		ST R
X DXDAW6W2 N7CTFE9R G9EJN9DW DUMSZGOP WIN32 PE GLCFKTON TGATNDBK EG3YER3E OFMSZGOP WIN32 PT6 RIWCYBLD TCKXCMWP M334XH27 FROBZWILP ORFO RYCYBLD TCKXCMWP M334XH27 FROBZWILP ORFO RXVW AR74GR6R LKQEFQSG 9XLQ7HQ2 HSQYQLPF ZCBGR	ID 6X NKCY EKY BYA GNY KXR 62R 62R	ST HR4 DAE 9FG WHM QBK 2CB 3NG	RENRABBY ALC323FP 6QCYY7K3 HA9Y7CWE DIMBZ8QP FNDBIMEP MBCYQLFF CHC736LA	8125C48QC A222M478 DCH883TB C983H9DW EG312EH38 H334X8427 9XLQ7HQ2 YTMC65	NGYDSN76 47 YRTYN3 ENCHTRIN BYCTFESR TGATNDBS TCKXCMNP LKOEFG56	2BGRETGH T9ABW3MT CHRMY3PA SXD3W6W2 8LCFRTQN RYWCYBLD RT4GR68	X P8 PTC	

Pencil and paper technique

Dates back to 1882 (Frank Miller, designing for telegraph machines)

One-Time Pad (OTP)



One-Time Pad (OTP)

- Ciphertext provides no information about the original message (beyond length)
 - Thus, OTP has property of Perfect Secrecy ☺
 - Eve has no idea if P_i was 0 or 1 Cannot be broken!
- But, Perfect Secrecy property is only true if: 8

One-Time Pad Problems

- One-Time Pad must be used only <u>once</u>!
 - Problem: Repeated use allows statistical comparisons easy to break
- One-Time Pad must be (cryptographically) random
 - Problem: Random number generation is hard/slow
- One-Time Pad must be shared between parties
 - Problem: Sharing must occur in advance of communication, out of band?
 - Both parties must keep pad secret
- One-Time Pad must equal length of plaintext
 - **7** Problem: Length!

Beyond the One-Time Pad

→ What do we use instead? Ciphers!

- ↗ Manageable key sizes ☺
- Methods to negotiate keys over the Internet with parties we've never communicated with before ^(C)
- Systems are more complex and lack the theoretical Perfect Secrecy property of OTPs 😕