Crypto Foundations



By Chad Parry <chad.parry@overstock.com>

Security Over Time



Caesar Cipher



Substitution Cipher





Frequency Analysis



Vigenère cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ AABCDEFGHIJKLMNOPQRSTUVWXYZ BBCDEFGHIJKLMNOPQRSTUVWXYZA C C D E F G H I J K L M N O P Q R S T U V W X Y Z A B D D E F G H I J K L M N O P Q R S T U V W X Y Z A B C EFGHIJKLMNOPQRSTUVWXYZABCD F F G H I I K L M N O P O R S T U V W X Y Z A B C D E G G H I J K L M N O P Q R S T U V W X Y Z A B C D E F H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G IIJKLMNOPQRSTUVWXYZABCDEFGH JJKLMNOPQRSTUVWXYZABCDEFGHI K K L M N O P Q R S T U V W X Y Z A B C D E F G H I J LLMNOPQRSTUVWXYZABCDEFGHIJK M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L N N O P Q R S T U V W X Y Z A B C D E F G H I J K L M 0 0 P Q R S T U V W X Y Z A B C D E F G H I J K L M N P P Q R S T U V W X Y Z A B C D E F G H I J K L M N O QQRSTUVWXYZABCDEFGHIJKLMNOP R R S T U V W X Y Z A B C D E F G H I J K L M N O P Q S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R T T U V W X Y Z A B C D E F G H I J K L M N O P Q R S U U V W X Y Z A B C D E F G H I J K L M N O P Q R S T V V W X Y Z A B C D E F G H I J K L M N O P Q R S T U WWXYZABCDEFGHIJKLMNOPQRSTUV XXYZABCDEFGHIJKLMNOPQRSTUVW YYZABCDEFGHIJKLMNOPQRSTUVWX Z Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Plaintext:ATTAC KATDA WNKey:LEMON LEMON LECiphertext:LXFOP VEFRN HR

Kasiski Examination

 Plaintext:
 CRYPT OISSH ORTFO RCRYP TOGRA PHY

 Key:
 ABCDA BCDAB CDABC DABCD ABCDA BCD

 Ciphertext:
 CSAST PKVSI QUTGQ UCSAS TPIUA QJB

 1234

1234 CSAS TPKV SIQU TGQU CSAS TPIU AQJB

Kerckhoffs's Principle

"The enemy knows the system." — Claude Shannon

The only secrets should be the keys.

Security Through Obscurity

You aren't as creative as you think you are.



Steganography



Image by John V Willshire

Automated Cryptanalysis

of shell		EverCrackv1.3.1 Open Source Crypto-Analysis Engine	- O ×
C:\CODING\EVERCR~1	\WINDOWS\DOS\bin>evercrac 3.txt	Program Convert Transposition Frequency Analysis Choose Language	Distancery
Cipher Text		Crack CODING\EVERCRACK\WINDOWS\BOR	RLAND\DEEP\10.TXT
1 18 21##110 21##135 14% 1 *\$\$ 1 27^#\$ 1508 ^6 88 3^(4&580\$4 7\$5\$ 14 %\$61143\$ ^6 &851448 8^(71v\$ 3^0\$ &^ 61)7& 1* 655\$ 0\$4 14% 65\$\$ 014 8^(15\$ 2718 21#0 8^(% 2187^(6)55\$\$% 2140 8^(61)7& &2^ &2718 21#0 8^(% 2187^(6)5\$\$% 9130 6!)7& 14% 8^(61) 4% #1v\$ 8\$= 21##13\$ *7^(&\$% 9130 6!)7& 14% 8^(018 %15 5(4 14% 8^(21## #1v\$ 1& #515* 12% 14% %15 14% 14% 65 9\$% 0148 8515* 65^8 4^2 2^(#% 8^(95 &^ &51%5 1## &75 %18* 65^8 &7143\$ &^ 8718 6^5 ^45 371433 j(*% ^45 37143\$ &^ 3A0\$ 9130 7555 1* 8^(4) 0\$4 14% &\$x# ^(5 \$45015* 6716 &716 818 8105 1(5 55* 968 875 2188 4555* 6105 4(5 5)) 818 8105 1(5 5) 968 758 2188 4555* 6105 4(5 5)) 818 8105 1(5 5) 968 758 2188 4555* 6105 4(5 5)) 8278 6^5 5 45 371435 j(*% 45 371435 & 4716 &758 105 4(5 5)) 818 8105 1(5 5) 968 758 2188 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6508 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6508 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6508 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6508 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6508 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 4555* 6105 4(5 5)) 8278 6^5 5 405 758 218 455* 6105 4(5 5)) 8278 6^5 5 405 758 218 455* 6508 5105 4(5 5)) 8278 6^5 5 405 758 218 455* 5105 4(5 5)) 8278 6^5 5 405 758 218 455* 5105 4(5 5)) 8278 6^5 5 405 758 218 455* 5105 4(5 5)) 8278 6^5 5 405 755* 5105 455* 5105 4(5 5)) 8278 6^5 5 405 755* 5105		Time [secs] 0.44 Decodes 1 Cipher Text dpaovba uhapvuhspaf ylspnpvbz iphz huk fvb jhss bz jyj	Clear Fields Otpuhsz fvb
[1]i am william wallace and i see a whole army of my countrymen here in defiance of tyranny you have come to fight as free men and free man you are what will you do without freedom will you fight two thousand against ten the veteran shouted no we will run and live yes wallace shouted back fight and you may die run and you will live at least awhile and dying in your bed many years from now would you be to trade all the days from this day to that for one chance just one chance to come back here as young men and tell our enemies that they may take our lives but they will never take our freedom		huk ayf av thri bz ilspici paz mvy vby vdu nvvk fla dlyl aol jyptpuhsz flz p ht h jyptpuhs tt jypti pz aoha vm jbypvzpaf tt jypti pz aoha vm qbknpun wlvwsi if doha aolf zhf huk aopur uva doha aolf svvr spri tf jypti pz aoha vm vbazthyapun fvb zvtlaopun aoha fvb dpss ulciy mvynpci ti mvy	-
		Plain Text Set Time Limit 5	D
		build bombs wage wars murder cheat and lie to us and try to make us believe its for our own	A
Time [secs]:	0.270000	good yet were the criminals yes I am a criminal my crime is that of curiosity my crime is that	
Decodes:	1 Enuron Consta Analuzia Espina	of judging people by what they say and think not	
Developer:	Corv Michael Boston [Dark Loose]	what they look like my crime is that of outsmarting	
are report	cory mender addrein [bark cogie]	you someting that you will never torgive me for	L
	AND MDYMEA DYCA Incom		<u>}</u>
C. CODERO (ETCNCK-1	THE REAL POINT ALLES		

Shown here: http://sourceforge.net/projects/evercrack/

Modern Cryptography







Image by Bo Allen

One-Time Pad Instructions

- Generate random numbers for key, *perfectly safely*.
- Exchange key with recipient, perfectly safely.
- Encrypt plaintext by addition with key.
- Dispose of key, perfectly safely.

Venona Project



Asymmetric Keys







Shopping Authentication



😣 🗐 🗊 Page Info - https://www	.overstock.com/ch	neckout?TID=NavCart
General Media Permissions	Security	
Website Identity		
Owner: Overstock.com I	DC.	
Verified by: VeriSign, Inc.		
		<u>V</u> iew Certificate
Privacy & History		
Have I visited this website prior t today?	⁰ Yes, 18	5 times
Is this website storing information (cookies) on my computer?	Yes	View Coo <u>k</u> ies
Have I saved any passwords for t website?	his No	Vie <u>w</u> Saved Passwords

Technical Details

Connection Encrypted: High-grade Encryption (3DES-EDE-CBC, 168 bit keys) The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

l®

RSA Key Example

- Choose random primes: p = 137, q = 131
- Calculate n = pq = 17947
- Choose small e = 3
- Solve for *d*: *de* mod lcm(p 1, q 1) = 1

 $\therefore 3d \mod 8840 = 1$

∴ *d* = 2947

- Public key: { *n*=17947, *e*=3 }
- Private key: { *n*=17947, *d*=2947 }

RSA Encryption Example

- Public key: { n=17947, e=3 }
- Private key: { n=17947, d=2947 }
- Message: m = "Hi" ≡ [72, 105] ≡ 9321
- Encrypt: $c = m^e \mod n$
 - $= 9321^3 \mod 17947$

= 9441

- Decrypt: $m = c^d \mod n$
 - $= 9441^{2947} \mod 17947$
 - = 9321

Public-Key Reliability

- Using the key incorrectly voids the warranty.
- Don't use the same key pair for both encryption and signing, unless your system gives you permission.
- The underlying factoring problem may be solvable.
- The TWINKLE device can brute-force keys.

Shor's Algorithm



Quantum Indeterminacy



Quantum Channels

Polarization	0	1		
+	↑	\rightarrow		
×	~	2		

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random basis	+	+	×	+	×	×	×	+
Sent polarization	ſ	\rightarrow	У	Ţ	У	7	7	\rightarrow
Bob's random basis	+	×	×	×	+	×	+	+
Received polarization	ſ	7	У	7	\rightarrow	7	\rightarrow	\rightarrow
Received bit	0	0	1	0	1	0	1	1
Shared secret key	0		1			0		1

Makarov's Hack



Image by "fatllama" on Flickr

Side Channel Attacks

Cryptographic proofs assume knowledge of all attack vectors.

Successful attackers will break the rules.

Acoustic Cryptanalysis





HAGELIN M-209 CIPHER MACHINE (GVG / PD)



Capacitor Hum



Image by Adi Shamir and Eran Tromer

Suitcase-Full-of-Money Attack



Image by "401(K) 2012" on Flickr

Rubber-Hose Attack



Image by Sam Ley "phidauex" on Flickr Overstock.com Tech Day 9/2012

Social Engineering



Image from http://www.smbc-comics.com/index.php?db=comics&id=2526 Overstock.com Tech Day 9/2012



Schneier's Law: "Any person can invent a security system so clever that she or he can't think of how to break it."

Never invent your own cryptography.