

Encryption v20.10

Jason A. Lord



“Cryptanalysis” for Incident Responders,

v20.10

Jason A. Lott, CEO
us Services, Ltd.

www.WeAreCyber.com





Crypto Background

- Cryptography vs Cryptanalysis
- Public-key
 - Diffie-Hellman
 - RSA
- Symmetric-key (shared)
 - DES
 - AES



Modes of Operation

- CBC
- LRW
- XEX
- XTS
- others...



AES

- Advanced Encryption Standard
- Substitution permutation network
- Fixed blocks (128 bit)
- Fixed keys (128, 192 or 256 bit)
- Process
 - Key expansion
 - Initial Round
 - Rounds
 - Final Round
- 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys



SubBytes

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

SubBytes

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

S

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$



ShiftRow

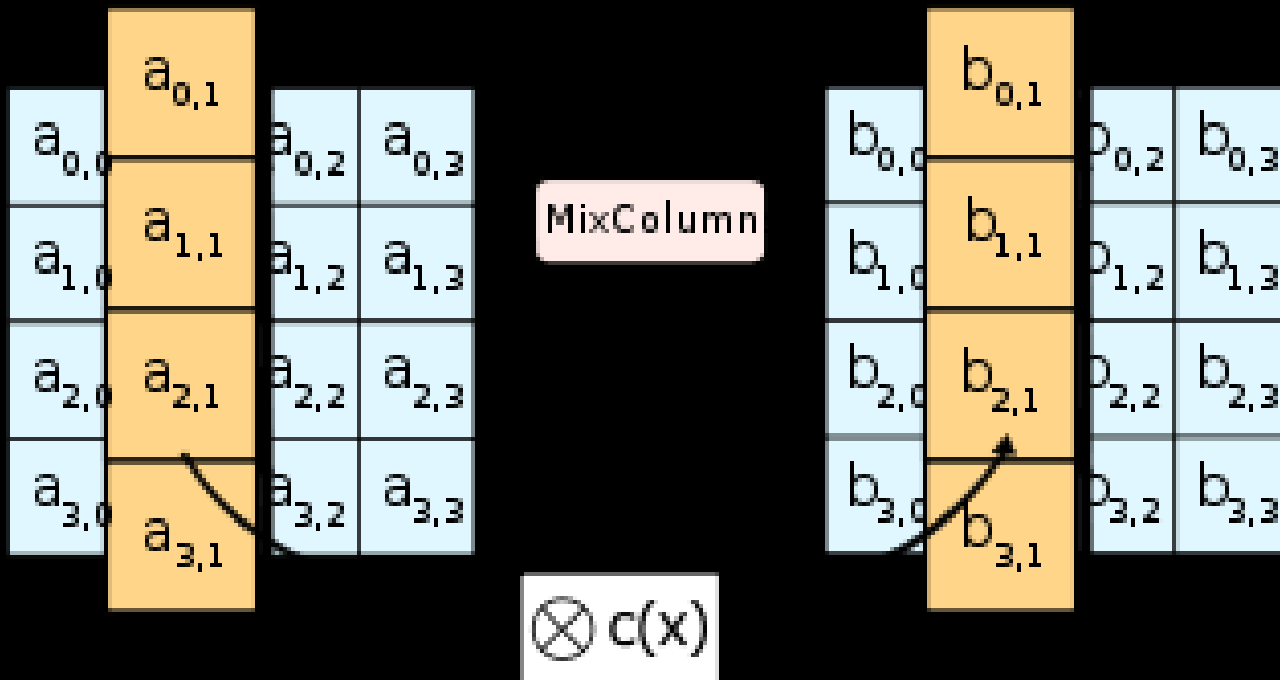
$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

ShiftRows

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,0}$
$a_{2,2}$	$a_{2,3}$	$a_{2,0}$	$a_{2,1}$
$a_{3,3}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$



MixColumn





Known Matrix

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2



$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

AddRoundKey

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$





Encryption Products

- Volume
- Whole Disk/Full Disk
- Compression/Encryption
- User Applications



Zip's

- WinZip, 7zip, et al
- AE-1 zip released in WinZip 9.0 (05/03)
- Three encryptions strengths
 - 128 (0x01), 192 (0x03), 256 (0x03) AES
- Compression method = 99
- File Format
 - Salt Value (8, 12, 16)
 - Password Verification Value (1 in 65,536)
 - Encrypted File Data (same as compressed data)
 - Authentication Code (the super-CRC)



Office Products

- Encryption Changes
 - 97-2003
 - 2007
 - 2010
- Password Types
 - Open
 - Protect
 - VBA



PDF's



Bitlocker

- Full disk encryption feature
 - Windows Vista Ultimate
 - Windows Vista Enterprise
 - Windows Server 2008
 - Windows 7 Ultimate
 - Windows 7
- 128 bit AES key, combined with a diffuser



Bitlocker

- Basic
 - TPM
- Advanced
 - USB
 - TPM + PIN
 - TPM + USB
 - TPM + USB + PIN (Vista SP1)

 - Pre-OS
 - Full Volume



Bitlocker

- Keys are generated via RNG > FIPS algorithm > random number
- Keys storage
- Key encryption (AES 256)

- Volume Master Key (VMK)
- Full Volume Encryption Key (FVEK)
 - Stored in OS volume



Bitlocker

- Always encrypted
- FVEVOL.sys
- Variable encryption sector size



Bitlocker

- The BIOS Parameter Block (BPB)
 - FVE-FS
- Viewable from physical drive
- Size, version, specific content



BitLocker

- Recovery Key
 - Offset 56(d), Length 4 bytes (Reversed)
 - Offset 60(d), Length 2 bytes (Reversed)
 - Offset 62(d), Length 2 bytes (Reversed)
 - Offset 64(d), Length 2 bytes (Forward)
 - Offset 66(d), Length 6 bytes (Forward)
- Coldboot attack
- Mount Volume



Successful Attacks

- Password Recovery (15)
- Password Guessing (3)
- Computer Online Forensic Evidence Extractor (COFEE) (1)
- Failures (6)
- 18 for 25 is not bad



PGPdisk

- Now part of Symantec
- 34 languages
- AES 128 or 256-bit keys



Trucrypt

- Removed at request of US Government



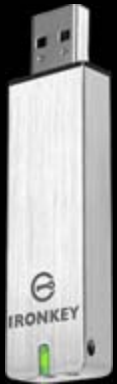


Crypto Hardware

- Iron Key
- Black Armor



IronKey



- 1GB – 32GB options
- AES 256 CBC encryption
- Password attempts
- Hardware by-pass protection
- Recover passwords



BlackArmor



- 500GB mobile safe
- AES 256 CBC encryption
- Password attempts
- Hardware by-pass protection
- SafetyDrill+
- Recover passwords



Cryptanalysis

- Not real cryptanalysis
- Attacks
 - Exhaustive search
 - Side channel attacks
 - cache-timing attack



Crypto Attacks

- Debugging
- PRNG issues
- Password by-pass
- Watermarking (CBC)



Passwords

- Human Nature
 - Personal
 - Sports
 - Region
- Breadcrumbs
- Sticky's
- RNG problems



Dictionaries/Wordlists

- 96 Printable Characters
- Language
- Entertainment
- Sports
- Geo/Region
- Books/Poems
 - Bible
 - Qu'ran
 - E. A. P.



Dictionaries/Wordlists

- Application
 - Permutation
 - Substitution
 - Unicode
 - Big/Little Indian
- Collection
 - Reusable
 - Small in size --- Huge in effort



Subject Profile

- Intelius
- Photos/Posters
- DoB's/PoB's/SSN's
- Facebook/MySpace/Pipl



Products

- AccessData PTK/DNA
- Elcomsoft Suite
- Accent Password Recovery
- OphCrack
- L0phtCrack
- John...



AccessData PRTK/DNA

- Go to Tool --- 90% success rate
- Office Suite
- Zips/Rars
- Distributed
- Rainbow Tables
- Dictionaries



Elcomsoft Suite

- Office Suite
- iPhone
- Internet Password
- Advanced Archives
- PDF
- DNA network
- \$49 - \$4999



Accent Office Password Recovery

- Microsoft Word, Excel and PowerPoint
 - 97-2003, 2007 and 2010
 - GPU support w/ multiple cards
- Bruteforce, Mask and Dictionary
- MS Access 97-2003 files
- Open, Modify and VBA passwords
- \$60 - \$350 for licenses

QUESTIONS???

jason.lord@d3-services.com

703-505-2524

www.WeAreCyber.com

