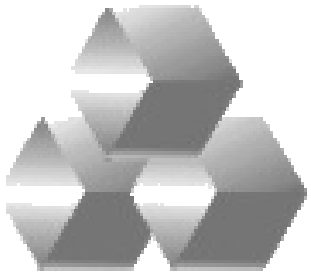


ElcomSoft

Presentation on on DEF CON Nine, July 13th - 15th, 2001
Alexis Park in Las Vegas, Nevada USA

eBooks security - theory and practice

http://www.elcomsoft.com

eBooks security - theory and practice

1. Foreword
2. PDF encryption
3. Standard security handler
4. Rot13 handler
5. FileOpen handler
6. SoftLock handler
7. Adobe Web Buy handler (PDF Merchant)
8. Acrobat eBook Reader EBX handler (formerly GlassBook)
9. Arbitrary handler (obtaining encryption key from PDF viewer)
10. Security flaw in Acrobat plug-ins certification

ElcomSoft

http://www.elcomsoft.com

Electronic Publishing

Advantages:

- Lower overhead publication and distribution cost
- Ability of instant worldwide distribution over the internet
- Many books in little physical volume
- Ability to search, highlight, underline, add annotations, bookmarks
- Hyperlinks

Disadvantages:

- Formats incompatibility
- Information in electronic form could be duplicated and transmitted, and there is no reliable way to take control over that processes.

Electronic Publishing/Reading Solutions

Software eBook leaders

- Adobe Acrobat PDF
- Microsoft Reader LIT

Dedicated reading devices

- RocketBook
- eBookMan Reader

Software eBook Compilers/Readers

- Activ E-Book
- E-Publisher Gold
- eBook Pro Compiler
- HTML2EXE
- E-Book Publishing Wizard
- eBook Generator
- Infinite Press Publisher
- WinEbook
- ...

ElcomSoft

http://www.elcomsoft.com

Related Internet resources:
http://www.ebookcompilers.com/

eBook Pro compiler

Short description (taken from www.ebookpro.com)

"eBook Pro", the only software in the universe that makes your information virtually **100% burglarproof!** It comes with a lifetime, money-back guarantee

"At Last, You Can Sell Information Online (And Make Thousands Of Sales Per Day) - Without The Danger Of Having Your Information Stolen And Resold By Others»

Actual features

All HTML pages and supplementary files are compressed with deflate algorithm from ZLIB

Compressed data are encrypted by XOR-ing each byte with every byte of the string “encrypted”, which is the same as XOR with constant byte

ElcomSoft
http://www.elcomsoft.com

Related Internet resources:
http://www.ebookpro.com/

PDF file structure

<PDF file> ::= <header> <body> <cross-reference table> <trailer>
<body> ::= <object> {<object>}
<object> :: <objectID> (<data> | <stream dictionary> <stream>)

Basic data types	**Example**	
Boolean	true	
Numeric	3.1415926	
Object reference	23 0 R	
Name	/ProcSet	
String	(Contents)	*
Stream	{binary data}	*

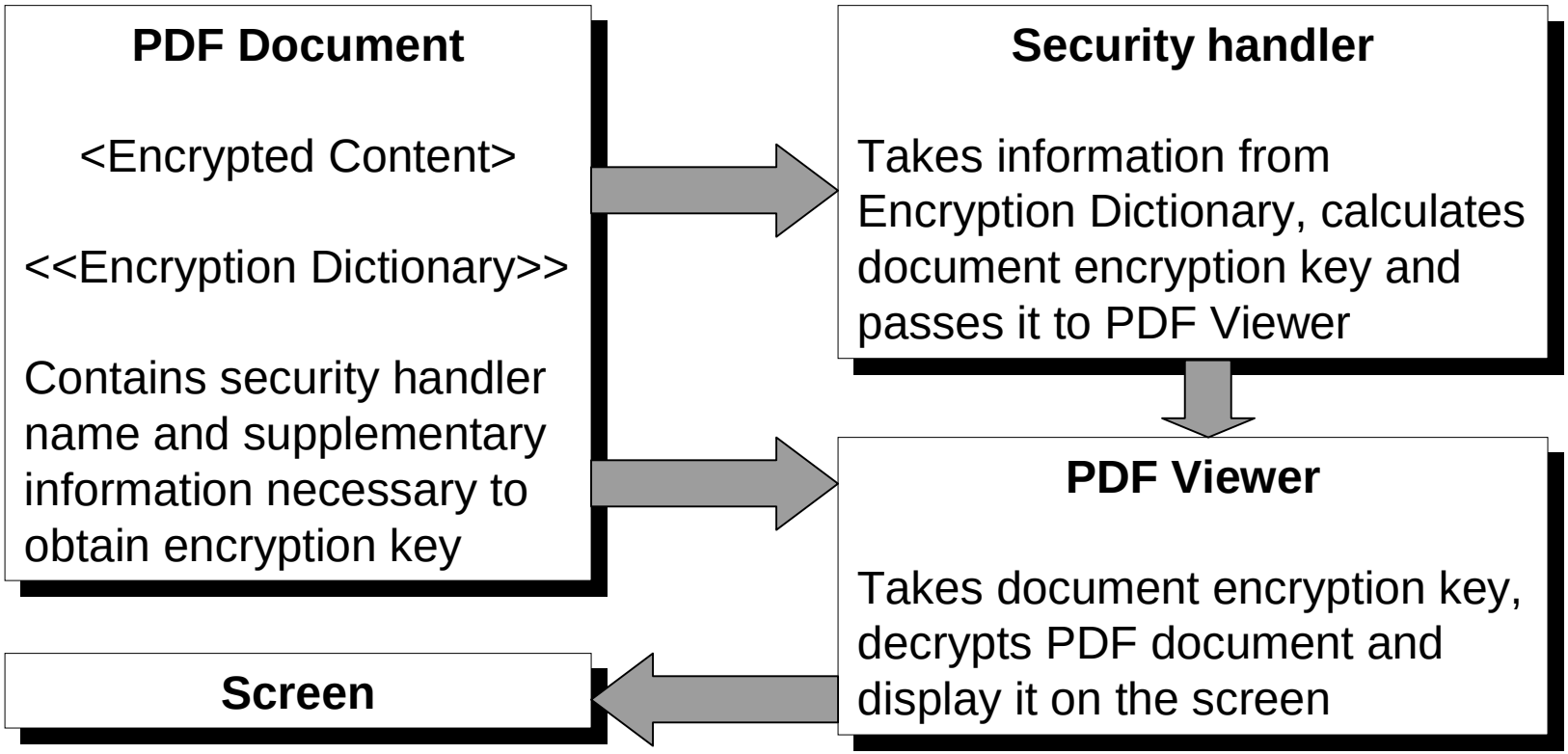
* - data could be encrypted

Complex data types	**Example**
Array	[23 0 R /XYZ null]
Dictionary	<</Name1 (Val1) /Name2 /Val2>>

ElcomSoft
http://www.elcomsoft.com

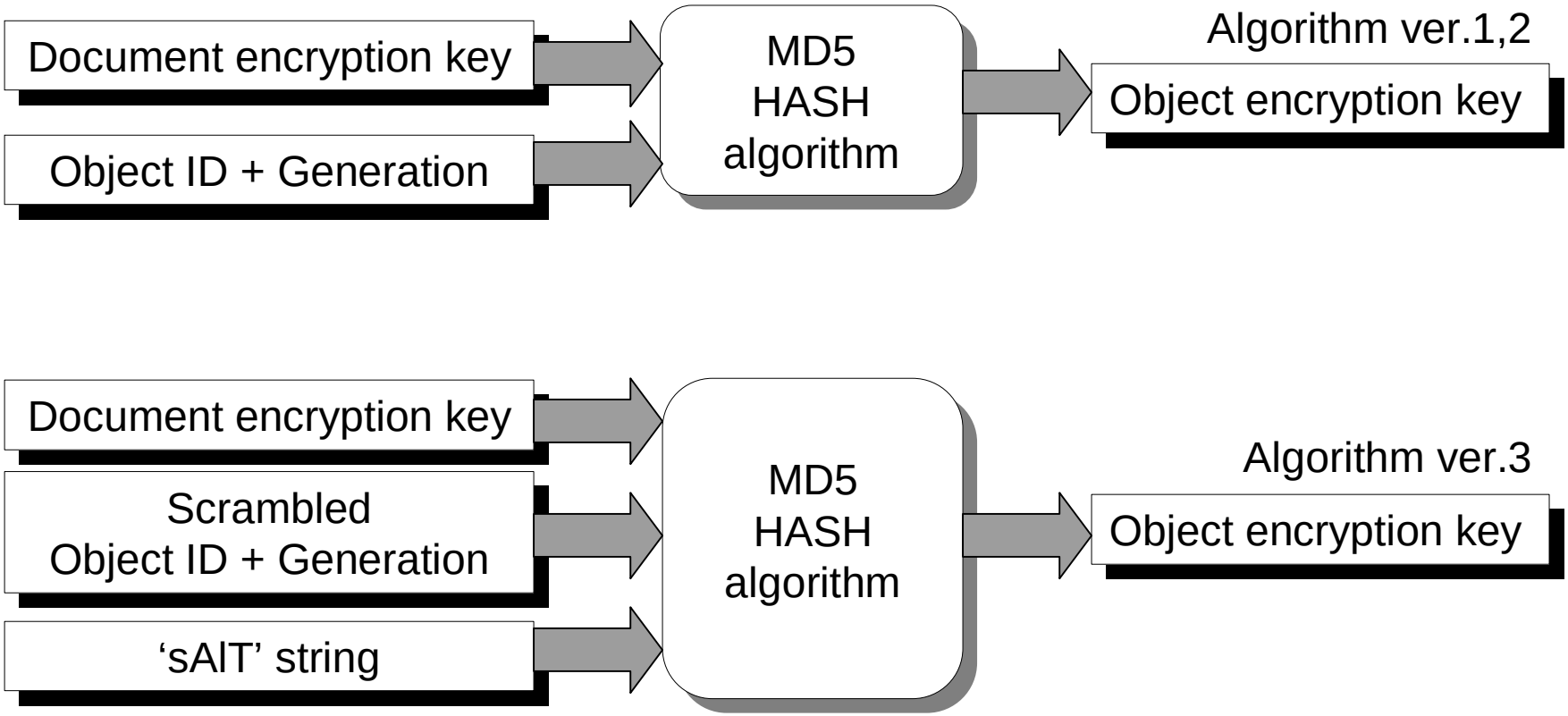
Related Internet resources:
http://www.adobe.com/products/acrobat/adobepdf.html

PDF file encryption



Related Internet resources:
http://www.adobe.com/products/acrobat/adobepdf.html

Object encryption key calculation



Related Internet resources:
http://www.adobe.com/products/acrobat/adobepdf.html

Standard security handler

Two passwords are supported:
- User (open) password – to open the document (with some restriction)
- Owner (security) password – to change security settings

Knowing either password is sufficient to decrypt the document

Possible restrictions, when opened with User password:

- Modifying the document's contents
- Copying text and graphics from the document
- Adding or modifying text annotations and interactive form fields
- Printing the document

New User password restriction, introduced in Acrobat 5:

- Form fill-in and sign document
- Text inspection and accessibility
- Page insertion, rotation,and deletion. Creation of bookmarks and thumbnails
- Low-quality printing only

ElcomSoft
http://www.elcomsoft.com

Related Internet resources:
http://www.adobe.com/products/acrobat/adobepdf.html

Standard security handler

Passwords per second on 450MHz Pentium III

Handler type \ Password type	User	Owner
Standard security handler 2	190,000 1×MD5 + 1×RC4	100,000 2×MD5 + 2×RC4
Standard security handler 3	3,250 51×MD5 + 20×RC4	1,610 102×MD5 + 40×RC4

Time necessary for complete key enumeration (40 bits key) on PIII-450

PCs \ total HDD	0 GB	128 GB	256 GB	384 GB	512 GB
1	960 hr	480 hr	240 hr	120 hr	60 hr
2	480 hr	240 hr	120 hr	60 hr	30 hr
3	320 hr	160 hr	80 hr	40 hr	20 hr
4	240 hr	120 hr	60 hr	30 hr	15 hr

Related Internet resources:
http://www.elcomsoft.com/apdfpr.html

Rot13 security handler

Short description

- Used by New Paradigm Resource Group (www.nprg.com)
- Protected documents costs about $3000 per copy
- Requires hardware dongle to operate

Actual features

- Clone of the “Rot13” sample plug-in, which supplied with Acrobat 4 SDK
- Uses fixed encryption key for all documents
- Key could be easily found as text string in the body of plug-in

Related Internet resources:
http://www.nprg.com/

FileOpen security handler

Short description (taken from www.fileopen.com)

- Developed by FileOpen Systems
- Supports pass-along prevention, document expiration, and controlled printing
- Adobe Selects FileOpen to Be An Acrobat 5 Security Partner
- Publisher's license costs $2500
- FileOpen and Acrobat 5.0 provide a complete, secure e-publishing solution

Actual features

- FileOpen Publisher 2.3 encrypts ALL documents with one fixed key
- FileOpen Publisher 2.4 uses variant keys, but encrypted document itself contains all necessary information to instantly calculate encryption key

Related Internet resources:
http://www.fileopen.com/

SoftLock security handler

Short description

- Developed by SoftLock Services, Inc. (www.softlock.com)
- Calculates unique SoftlockID Number based on HDD volume ID
- Requires password which matches SoftlockID to open the document
- Password is used in document key calculation

Actual features

- Unlocking password is exactly 8 characters
- Each character converted to one hexadecimal digit
- Two characters are used for integrity checking
- Effective password length is only 24 bits
- Correct password could be found by calling not optimized checking routine in 30 hours on 450 MHz CPU

Related Internet resources:
http://www.softlock.com/

Adobe WebBuy (PDF Merchant)

Short description

- License (.RMF file) is required to open the document
- License consist of:
  - Signed certificate with Publisher's RSA Public key
  - One or more pairs of some ID (like CPU ID, USER ID, UTC, …) and encrypted document key, associated with that ID. Different pairs are combined with "AND" and "OR" operators
  - Document permissions
  - Data to check license validity

- Two RSA Public keys owned by Adobe (1024 bit and 912 bit in length) are involved in license verification and document key calculation
- It is impossible to generate valid certificate without having access to RSA Private keys, owned by Adobe
- It is possible to calculate document key and decrypt the document if both PDF and matching RMF file are available

Related Internet resources:
http://pdfmerchant.adobe.com/

Adobe's Acrobat eBookReader (formerly GlassBook)

Short description

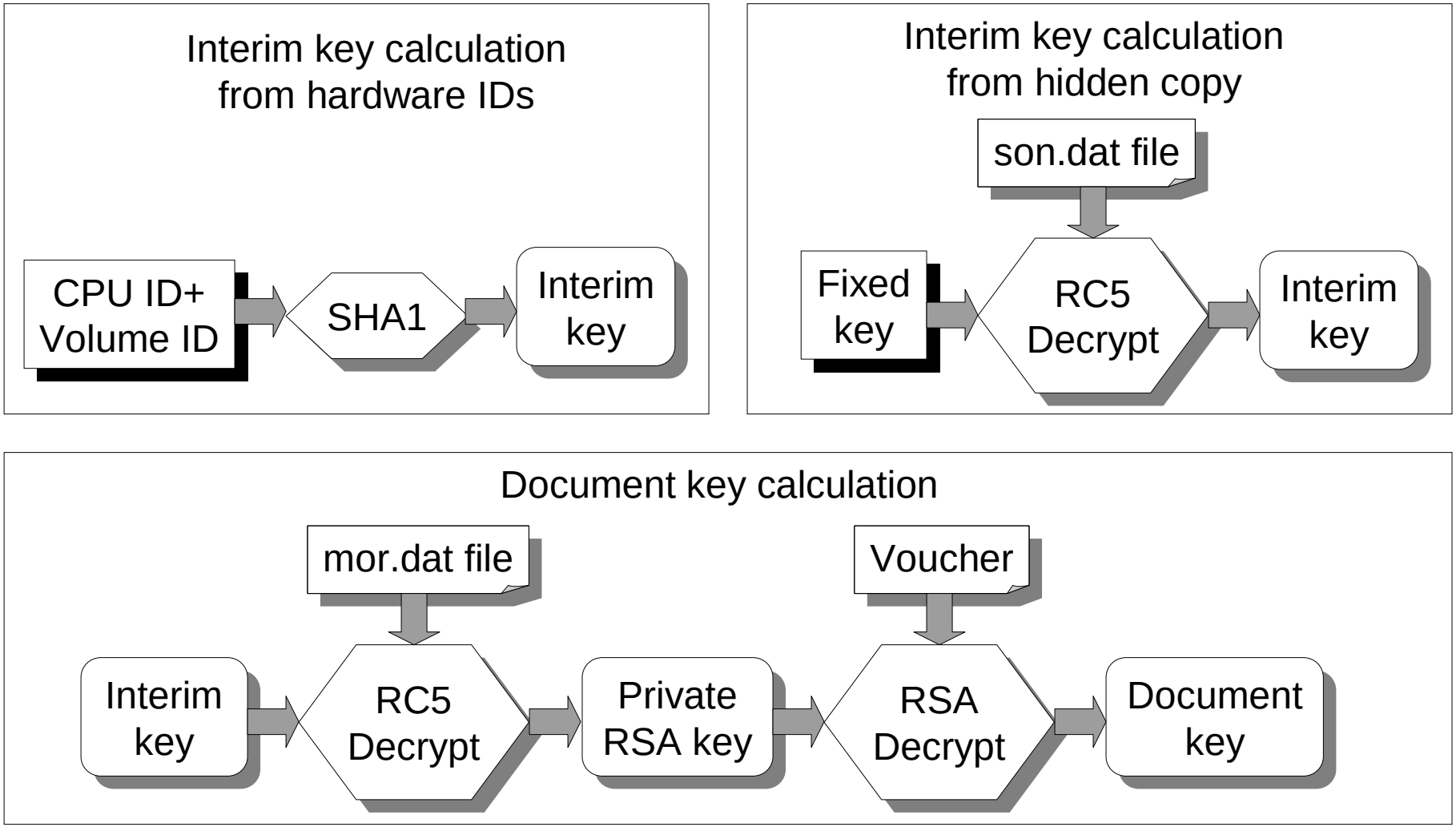
- Implements Electronic Book Exchange (EBX) protocol
- RSA keys pair is generated during activation
- Public key is registered on content server, while Private is retained by Reader
- Document key encrypted by Public key and stored in Voucher
- Voucher contains information about document permissions, expiration, …
- Voucher is signed with HMAC protocol

Brief analysis

- Voucher could not be falsified without knowing the Document key
- Document key could not be calculated without knowing the Private key
- Private key is stored somewhere on local computer
- After obtaining the Document key it is very easy to create Voucher with any permissions and for any computer

Related Internet resources:
http://www.ebxwg.org/
http://www.adobe.com/products/contentserver/main.html

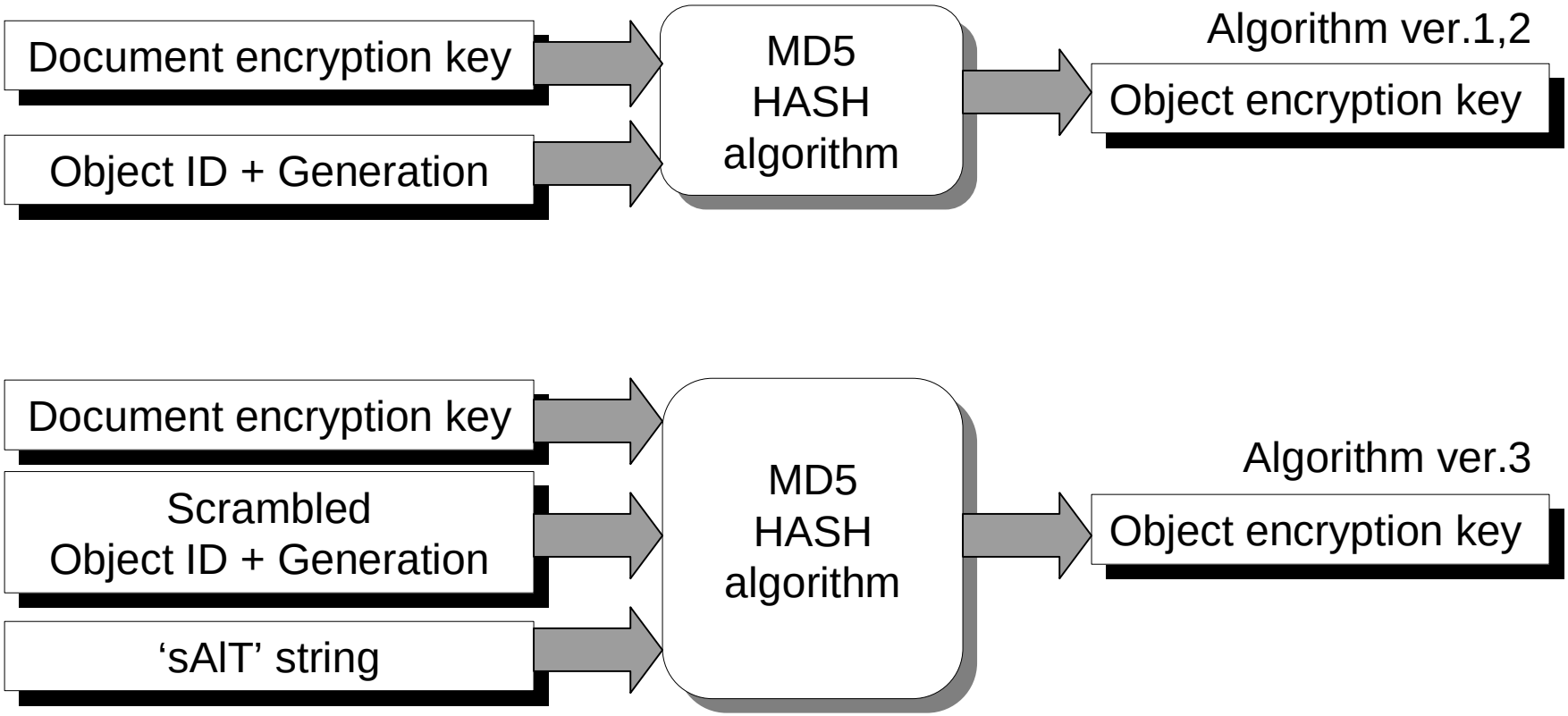
Adobe's Acrobat eBookReader (formerly GlassBook)



ElcomSoft
http://www.elcomsoft.com

Related Internet resources:
http://www.adobe.com/products/contentserver/main.html

Object encryption key calculation



Related Internet resources:
http://www.adobe.com/products/acrobat/adobepdf.html

Obtaining encryption key from PDF viewer

Anti reverse-engineering measures in PDF viewers

Application name	Code encryption	Debugger detection	Code integrity checking
Acrobat 4	No	No	No
Acrobat 5	No	In DocBox plug-in	No
eBook Reader	PACE InterLok	PACE InterLok	No

How to find code of MD5 functions

- MD5_Update function resides not far from MD5_Init function, which uses constants 0x67452301, 0xEFCDAB89, 0x98BADCFE and 0x10325476
- MD5_Update often called just after call to MD5_Init function
- MD5_Update or some function called from MD5_Update uses 64 constants defined in MD5 specification

Security flaw Acrobat plug-ins certification mechanism

Why to certify plug-in

- Only certified plug-ins will be loaded by Acrobat Reader
- In some cases (e.g. when opening document protected with WebBuy or DocBox) only plug-ins certified by Adobe are permitted to be loaded

How to certify plug-in

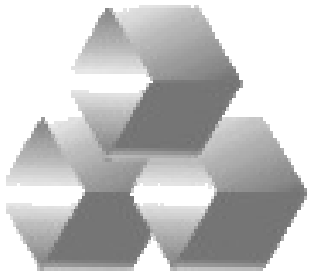
- Sign Reader Integration Key License Agreement with Adobe
- Pay $100 to obtain Reader Certification digital certificate from Adobe
- Use this certificate to Reader-certify any plug-in

How certificate validity is checked

- Only data from PE Header is used for checking

How to bypass plug-ins certificate checking

- Modify code of any plug-in certified by Adobe to load non-certified plug-in and pass control to it. Take care to not modify data in PE header



ElcomSoft

Presentation on on DEF CON Nine, July 13th - 15th, 2001
Alexis Park in Las Vegas, Nevada USA

eBooks security - theory and practice

http://www.elcomsoft.com