A Review of Advancements in Code Breaking and Password Recovery Technology

Code Breaking and Digital Forensics

FBI Supervisory Special Agent
Chris Beeson
Laboratory Director
Silicon Valley Regional Computer Forensic Laboratory
Menlo Park, CA
cbeeson@fbi.gov
www.rcfl.gov

Course Content

- Basic concepts in Cryptography
- Keyspace Dilemma
- PRTK
- Rainbow Tables
- Other Code breaking tools

What is Cryptography

- Cryptography: The art and science of keeping messages/information secure
- Encryption: Transformation of data into unreadable form
- Decryption: Reverse of encryption

Applied Cryptography 2nd Addition – Bruce Schneier / RSA Laboratories FAQs about Cryptography Version 3 - 1996

Types of Encryption

- Access Protection
  - Not encrypted, just locked
- Data obfuscation
  - Encryption by way of scrambling (ROT13)
  - Trillian
  - XOR
- Data encryption
  - Crypto systems

Password States

- Not stored
  - Application uses authentication sequence to verify (ie Word/Excel)
- Stored by User
  - Application offers to store, then obfuscate or encrypt (IE, Yahoo, Netscape)
- Stored by Application
  - EFS

Password Types

- Open/Modify Passwords (Word/Excel)
- Unlock
  - No encrypt, needed to open file (early Quicken)
- User/Master (PDF)
- Administrator
- Password archives
  - PasswordSafe, PasswordsPlus, etc

Terminology

Function

Salt

FEK

Keyspace

Array

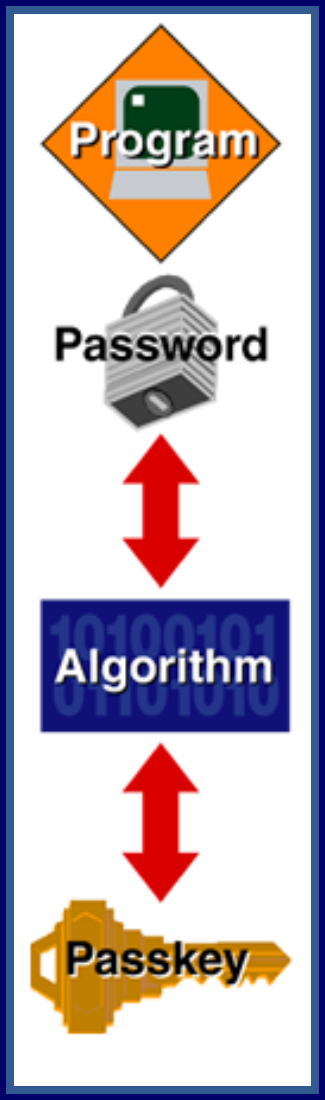
Plain Text

Cipher Text

Hash

- Hash Function
  - Variable length data stream = fixed length number
  - Must be reproducible with same data
  - Cannot be reversed (number back to original data)
  - Also called Message Digests (ie md5)

What is a Hash Function?



WINDOWS LOGON

CAT

MD4 / SHA

= A2D3C1AE4FD2EAC213DE45FA2DEC2AE2

Terminology

Function

Salt

FEK

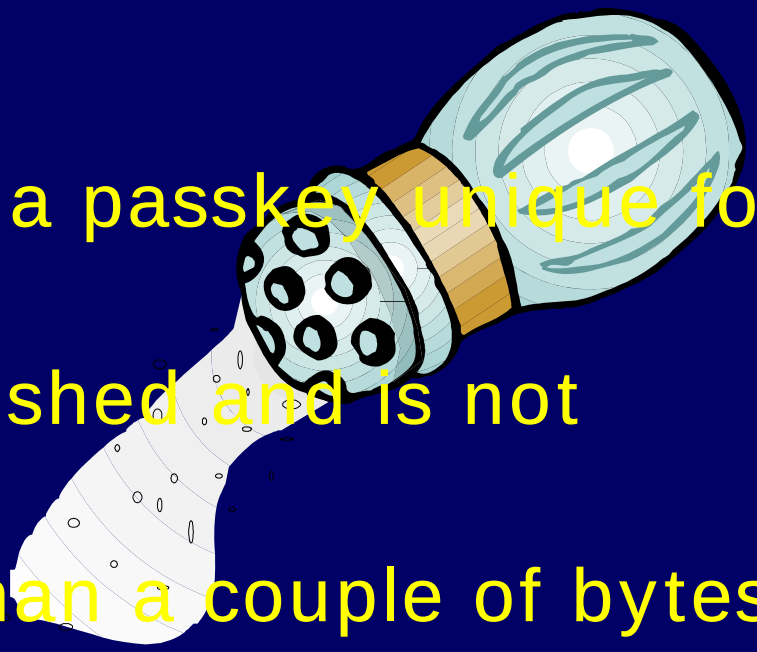
Keyspace

Array

Plain Text

Cipher Text

Salt



- Salt is used to make a passkey unique for each user/machine
- Salt is normally published and is not secret
- Salt is rarely more than a couple of bytes in size

Two Users – Same Password - With Salt:

User 1 cat = f3fca383b05f665ff43244ecdecfe959

User 2 cat = ccd15a3c85d28019fb3ef173f7ff344a

Terminology

Function

Salt

FEK

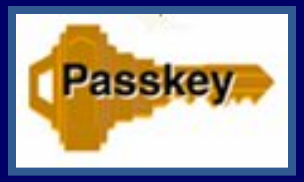
Keyspace

Array

Plain Text

Cipher Text

*F*ile *E*ncryption *K*ey



+ SALT

+

=

9o2GrDE398fD7ipR3

You get the idea !

Terminology

Function

Salt

FEK

Keyspace

Array

Plain Text

Cipher Text

Keyspace Values

Key: **Any One of a Larger Number of Values**
Keyspace: **Range of Possible Values**

(this can get big!)

20	1,048,576
30	1,073,741,824
32	4,294,967,296
33	8,589,934,592
40	1,099,511,627,776
50	1,125,899,906,842,620
56	72,057,594,037,927,900
60	1,152,921,504,606,850,000
70	1,180,591,620,717,410,000,000
80	1,208,925,819,614,630,000,000,000
90	1,237,940,039,285,380,000,000,000,000
100	1,267,650,600,228,230,000,000,000,000,000
110	1,298,074,214,633,710,000,000,000,000,000,000
120	1,329,227,995,784,920,000,000,000,000,000,000,000
128	340,282,366,920,938,000,000,000,000,000,000,000,000
160	1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000

Keyspace

Key Space Calculation Spreadsheet	
Key Space (# of bits)	40
Size of Key Space	1,099,511,627,776
Keys Tested Per Second	500,000
# of Machines	1
Time (in seconds)	2,199,023
Time (in hours)	610.840
Time (in days)	25.45
Time (in years)	0.070

Terminology

Function

Salt

FEK

Keyspace

Array

Plain Text

Cipher Text

Array

An Array is used by cryptographic systems to generate bit streams used to encrypt and decrypt data.

A random bit is used with a “Exclusive Or” (XOR) algorithm that switches the bits that comprise the data.

Terminology

Function

Salt

FEK

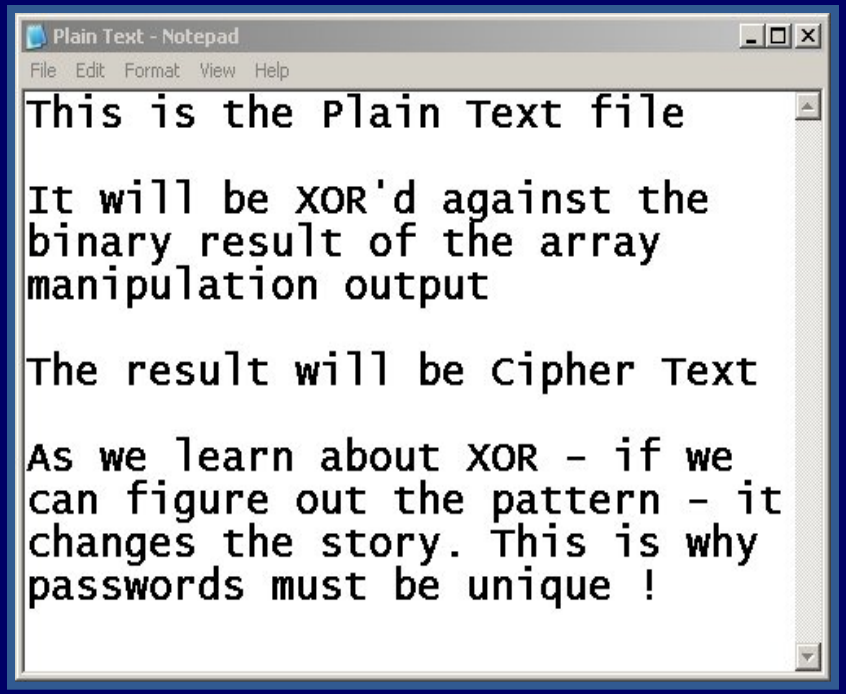
Keyspace

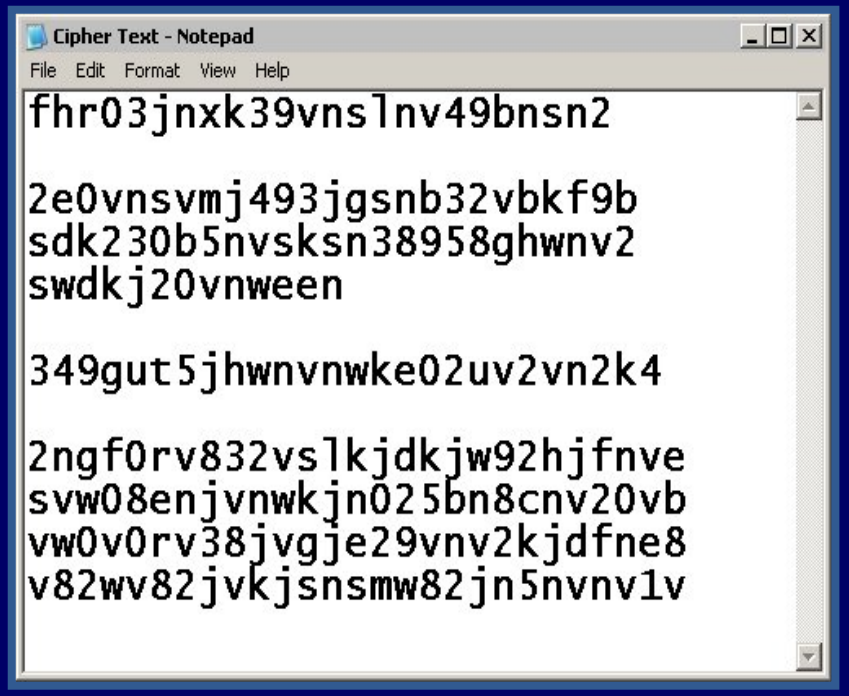
Array

Plain Text

Cipher Text

Plain Text → Cipher Text





1010010000101010011

(array value)

PT ^ array value = CT

Crypto System

Password

Algorithm

MD5 Hash, SHA Hash ??

40 bit

Passkey

40 bit

Algorithm

MD5 Hash, SHA Hash ??

FEK

RC4

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

0101010101011

^ PT

Plain Text - Notepad

```
This is the Plain Text file

It will be XOR'd against the
binary result of the array
manipulation output

The result will be Cipher Text

As we learn about XOR - if we
can figure out the pattern - it
changes the story. This is why
passwords must be unique !
```

Cipher Text - Notepad

```
fhr03jnxk39vnslnv49bnsn2

2e0vnsvmj493jgsnb32vbkf9b
sdk230b5nvsksn38958ghwnv2
swdkj20vnween

349gut5jhwnvnwke02uv2vn2k4

2ngf0rv832vslkjdkjw92hjfnve
svw08enjvnwkjn025bn8cnv20vb
vw0v0rv38jvgje29vnv2kjdfne8
v82wv82jvkjsnsmw82jn5nvnv1v
```

The Key Space and Password Space Dilemma

Code Breaking Tools

Password Cracking

Ability to recover passwords from well-known applications

- Decrypt files, folders, and hard drives
- Gain access to files protected by the Microsoft Encrypted File System (EFS)

Distributed Code Breaking

Ability to recover passwords and/or keys using:

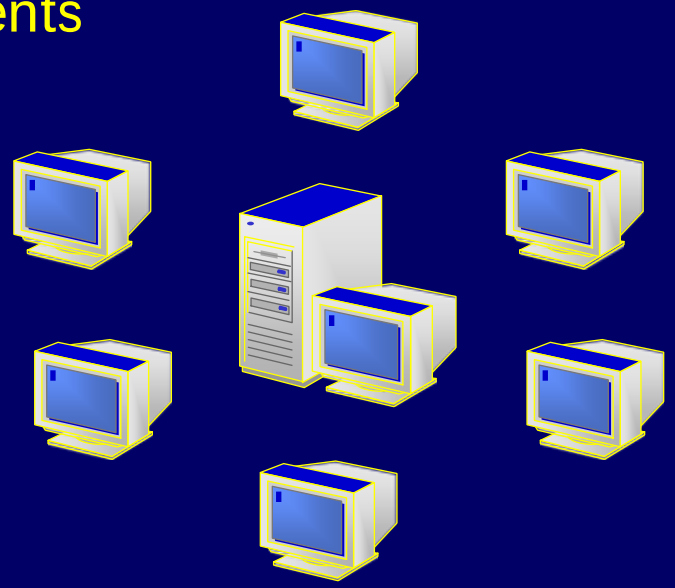
- Brute-Force attacks - Key-Space attacks - Pass-phrase attacks

– One system manages many Clients

– Distributed code breaking to many clients

- Apple Macintosh
- Linux
- UNIX
- Windows

– Uses 'Idle Process' time

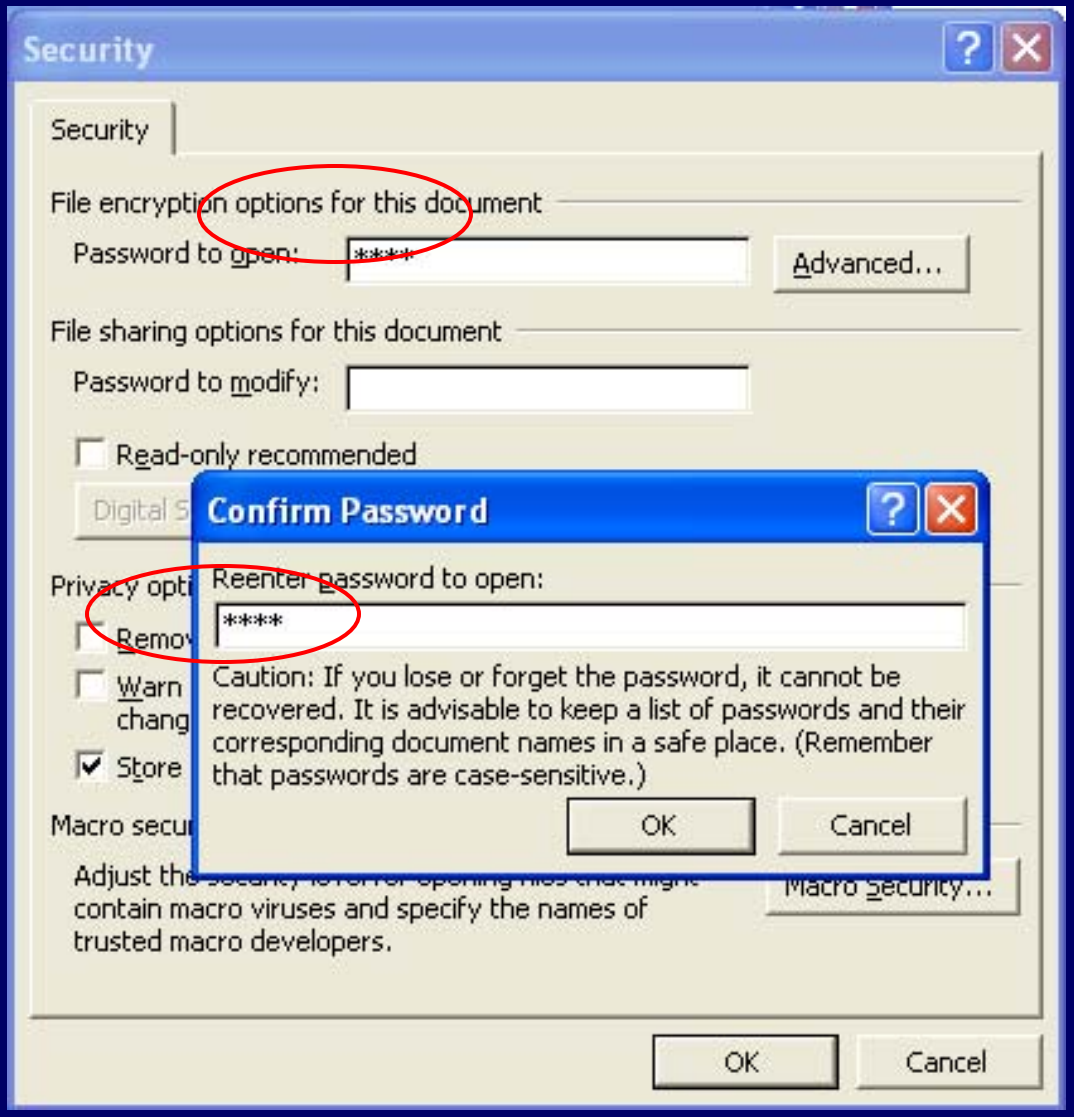


Attacking the RC4 Implementation in MS Office

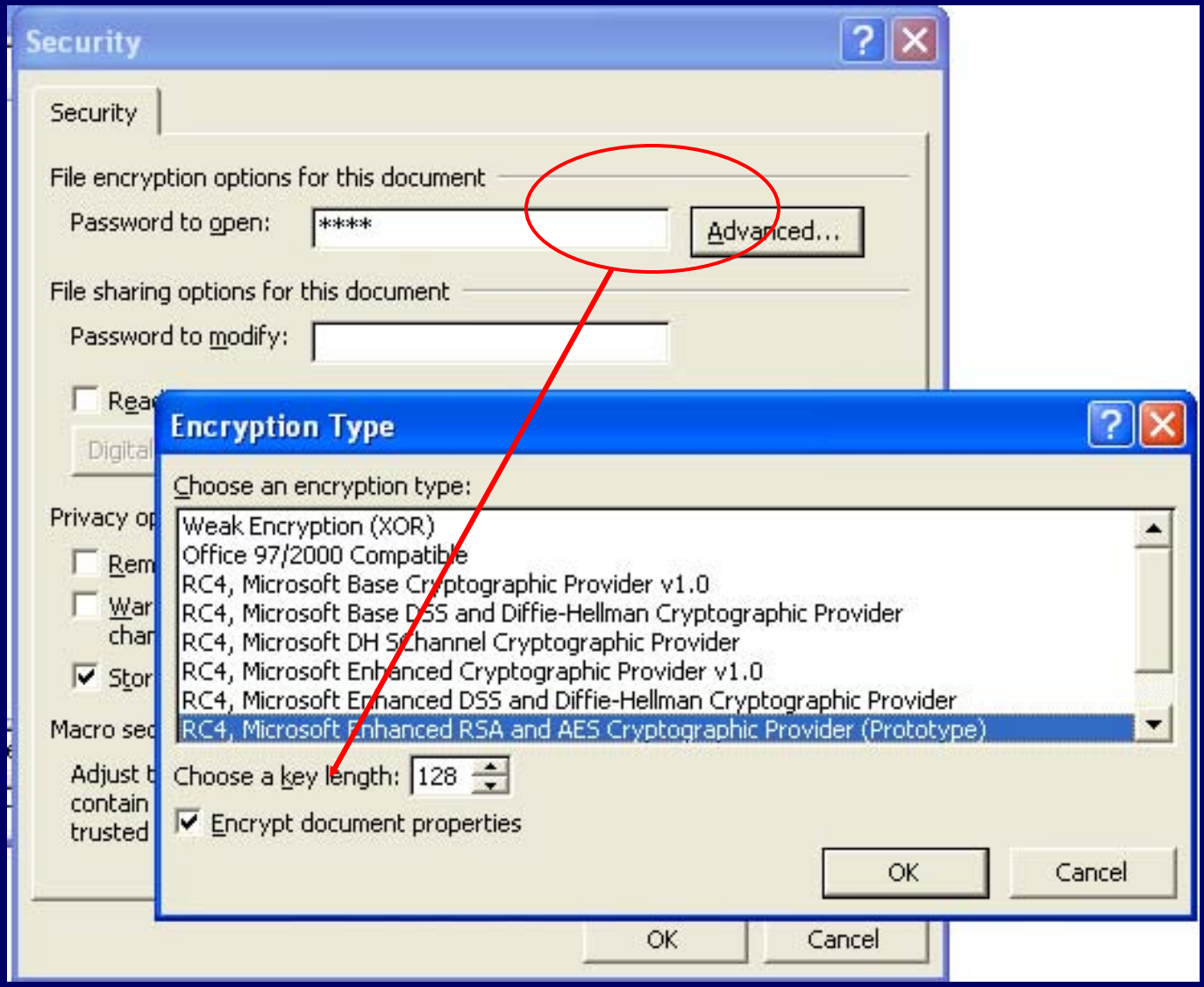
Microsoft Office 40-bit Encryption

- Due to U.S. Export laws, MS Office 97 and later versions use 40-bit FEK to initialize RC4 symmetric encryption algorithm.
- An exhaustive key space attack of a 40-bit key using a 25 computer distributed network attack (DNA) takes 24+ hours

MS Word – 40 bit Encryption



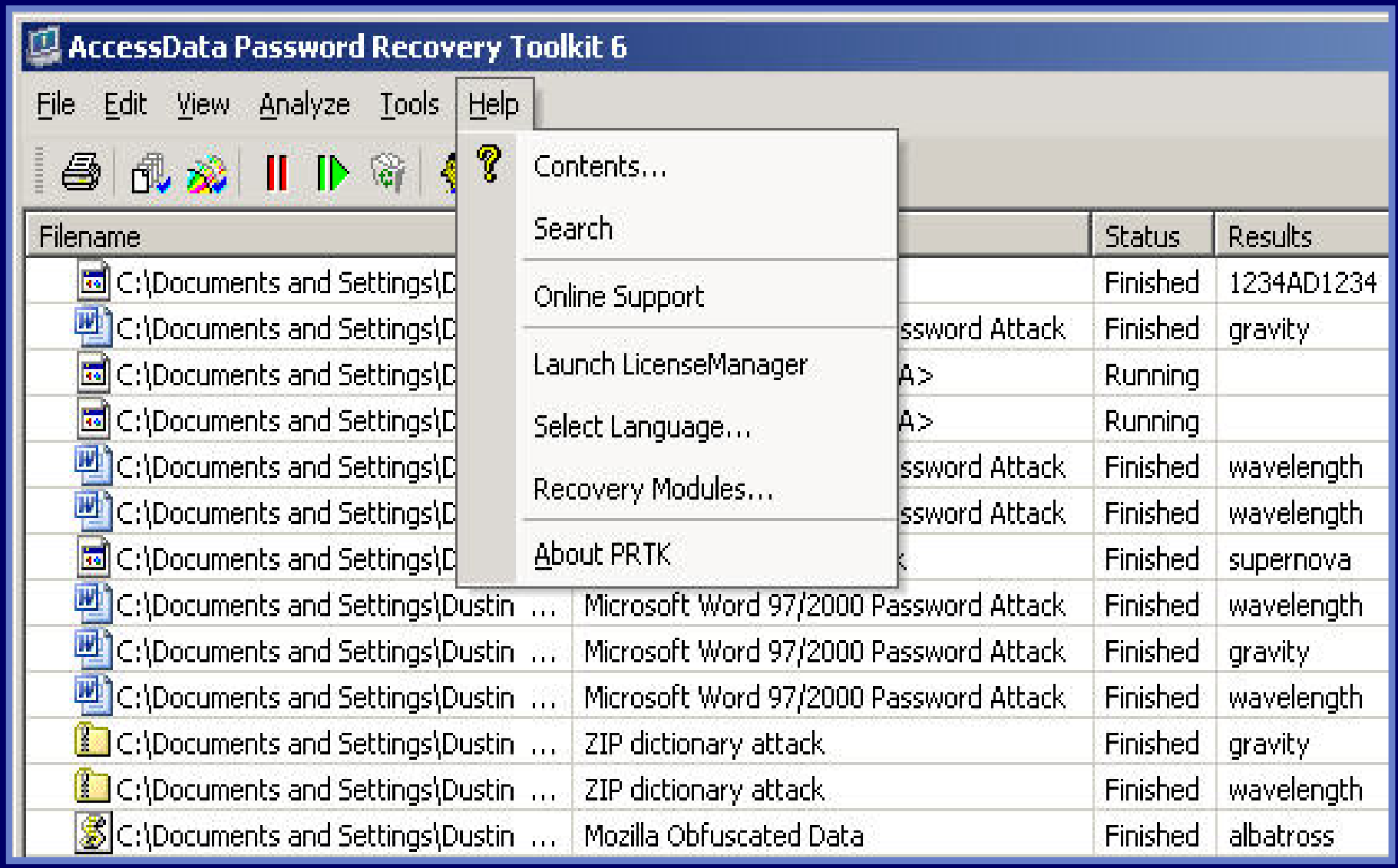
MS Word Advanced Encryption Option



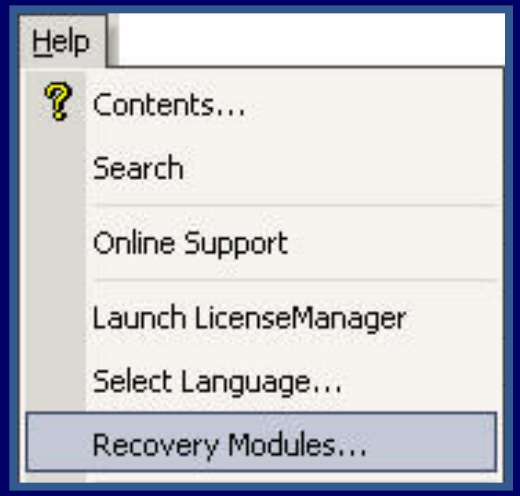
Code Breaking Tools

- AccessData
  - Password Recovery Tool Kit (PRTK)
  - Distributed Network Attack (DNA)

PRTK Overview



Recovery Modules



Module Name	Display Name	Attack Types	Supported Products
Access	MS Access Password Module	decryption	Product Name: Microsoft Access Versions supported: *Unknown*
ACT	ACT! Password Module	decryption	Product Name: ACT! Versions supported: 1 - 4 2000 5 - 6
AIM	AIM Password Module	dictionary	Product Name: AOL Instant Messenger Versions supported: Through 5.5
AmiPro	AmiPro Password Module	dictionary	Product Name: Ami Pro Versions supported: *Unknown*
AOL	AOL Password Module	keyspace decryption	Product Name: AOL Versions supported: 8.0 - 9.0
Approach	Lotus Approach Password Module	decryption	Product Name: Lotus Approach Versions supported: Through 97
ARJ	ARJ Password Module	dictionary keyspace	Product Name: ARJ Versions supported: Through 2.82
Ascend	Ascend Password Module	decryption	Product Name: Ascend Versions supported: *Unknown*
BestCrypt	BestCrypt Password Module	dictionary	Product Name: BestCrypt Versions supported: 4.x - 7.x

Some up front knowledge might make a difference !!

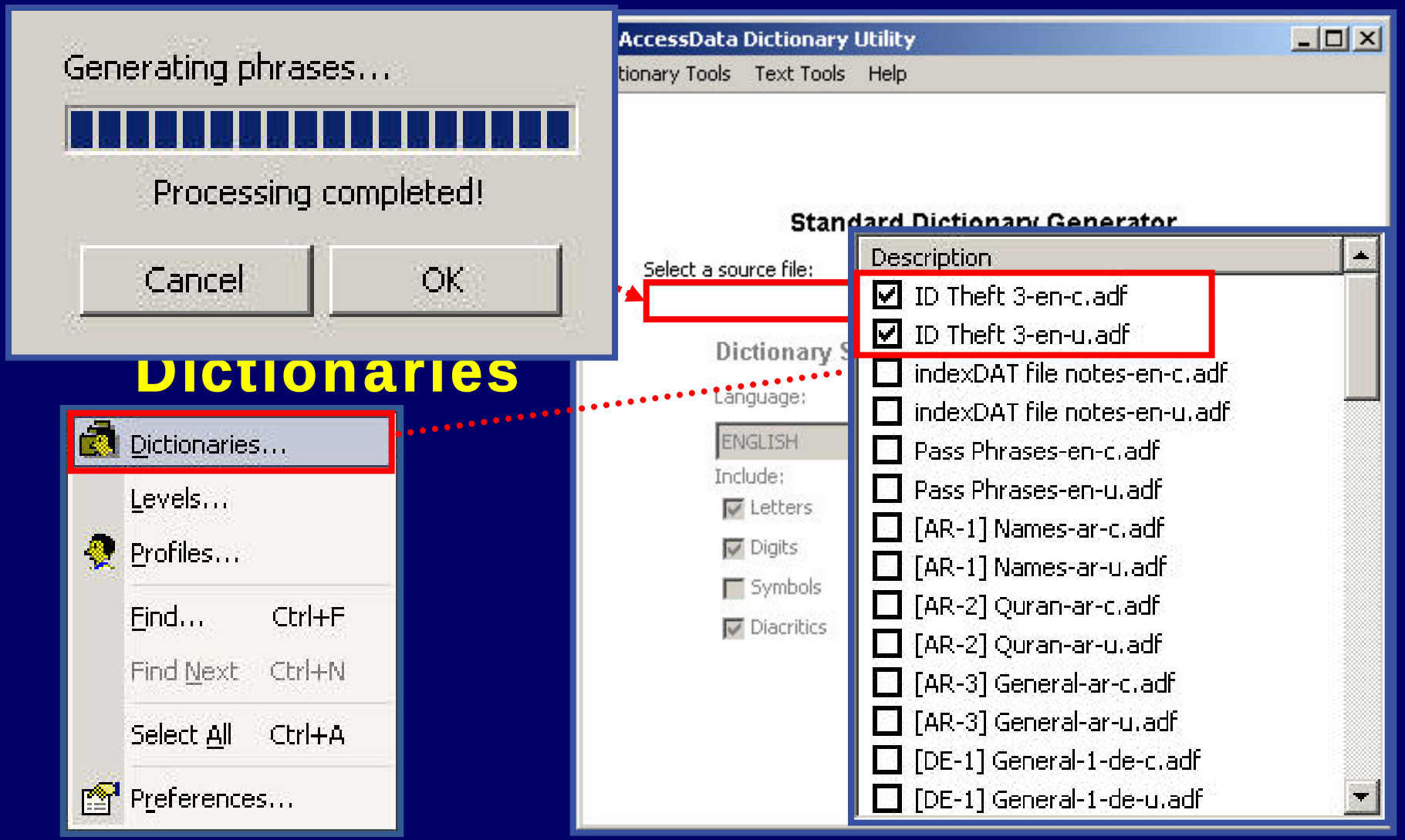
ABICoder	InvisibleSecrets	ProtectedRegistry
Access	Justsystem	ProWrite
ACT	Kaikei	PST
AIM	KeePass	PWL
AmiPro	Kremlin	QuattroPro
AOL	Lockit	Quickbooks
Approach	Lotus123	Quicken
ARJ	MaxCrypt	RARPassword
Ascend	MessengerPlus	SafeHouse
Ashampoo	Money	SAMFile
BestCrypt	MozillaMasterPassword	Scheduler
BPFTP	MozillaProtectedData	ScreenSaver
CDLock	MSBackup	SecretStuff
CheckWriter	MSMail	SecureIT
CodedDrag	MSNMessenger	SiFEU
crypt	MYOB	SourceSafe
Cryptainer	NetscapeMail	Steganos
CryptaXix	office	STools
Cryptext	Omziff	SymantecQA
CuteFTP	OpenOffice	VBA
DataPerfect	Organizer	VersaCheck
dBASE	Palm	Whisper
DriveCrypt	Paradox	WinZip9
DriveCryptPP	PasswordPal	WordPerfect
EasyCrypto	PasswordSafe	WordPro
EFS	PCEncrypt	WS_FTP
EMF	PDF	XPCredentials
FileMaker	PFX	YahooMessenger
Hello	PGP	ZIP
ICQ	PGPDisk	

- Working Smarter rather than Harder!

Dictionary Attacks

- User Created – Inside/Outside PRTK
- Dictionaries
  - Common – Common English words
  - Passwords – Password lists (golden dictionary)
  - Crime – Sex and drugs
  - Misc – Keyboard combinations
  - Names – Common names
  - General – Webster like
  - Unicode

Dictionary Creation



What is a Level?

- Level Technology – PRTK/DNA
- Primary Dictionary Search
  - rabbit
  - RABBIT
  - Rabbit
  - rABBIT
- 1abduct
- Toabduct
- abduct123

Prefixes

Postfixes

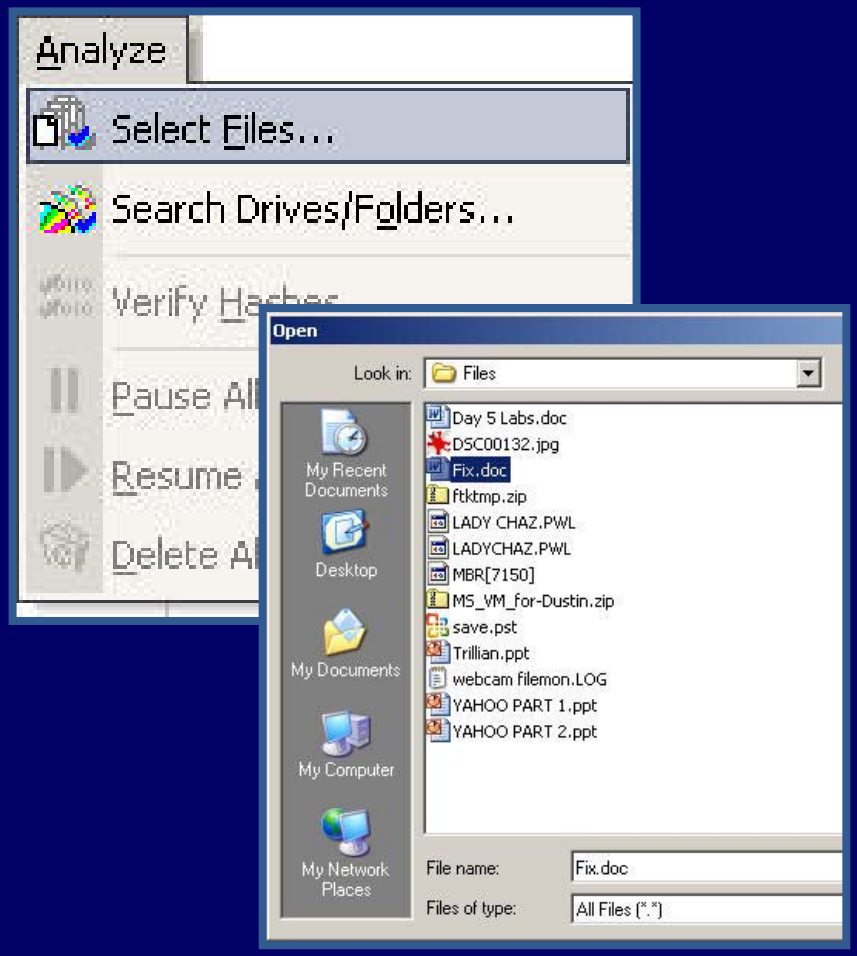
Word in a Word

Concatenation

Markov

Reverse

Starting a Job



OR

FIX.DOC

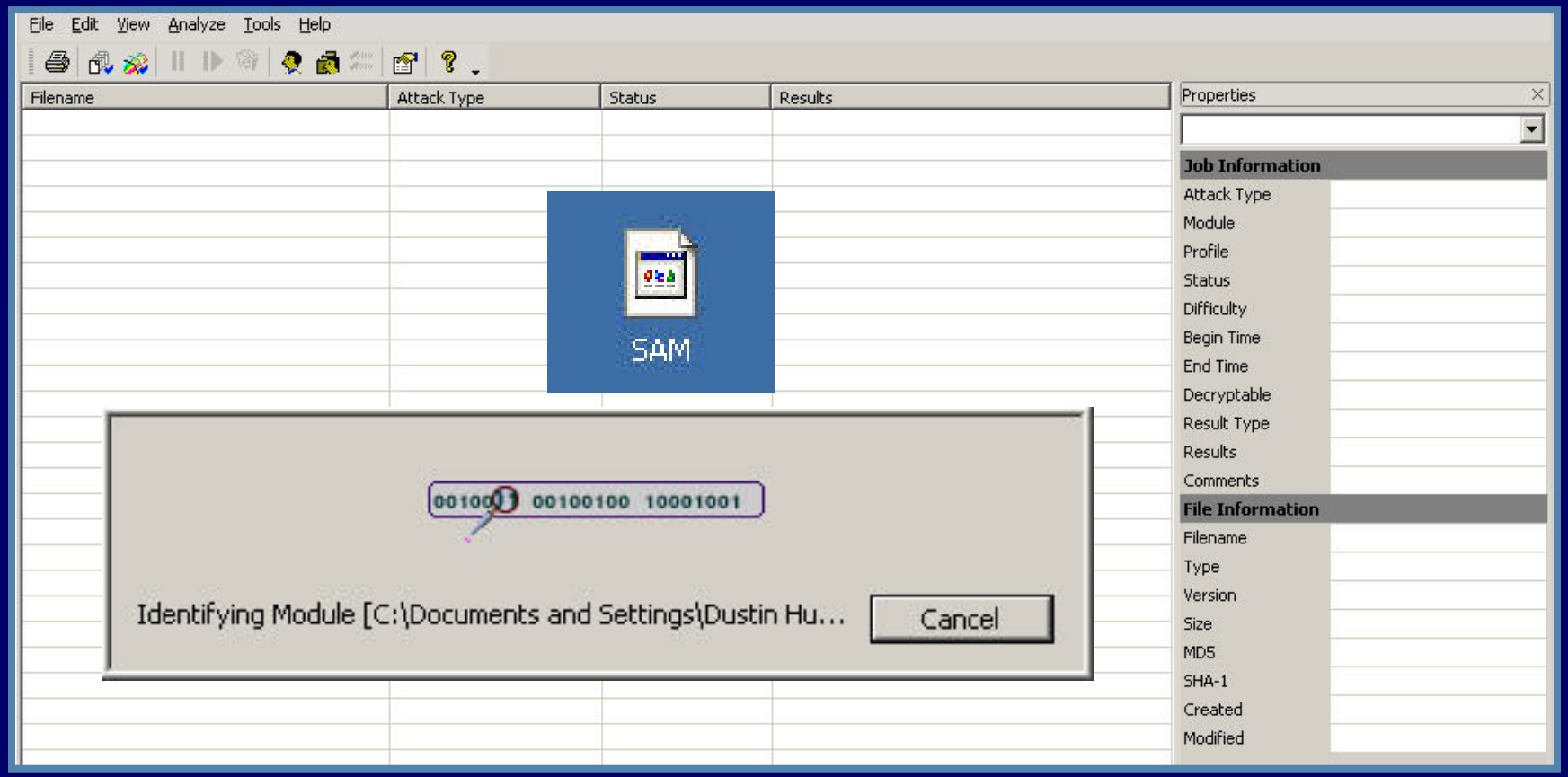
DRAG

D
R
O
P

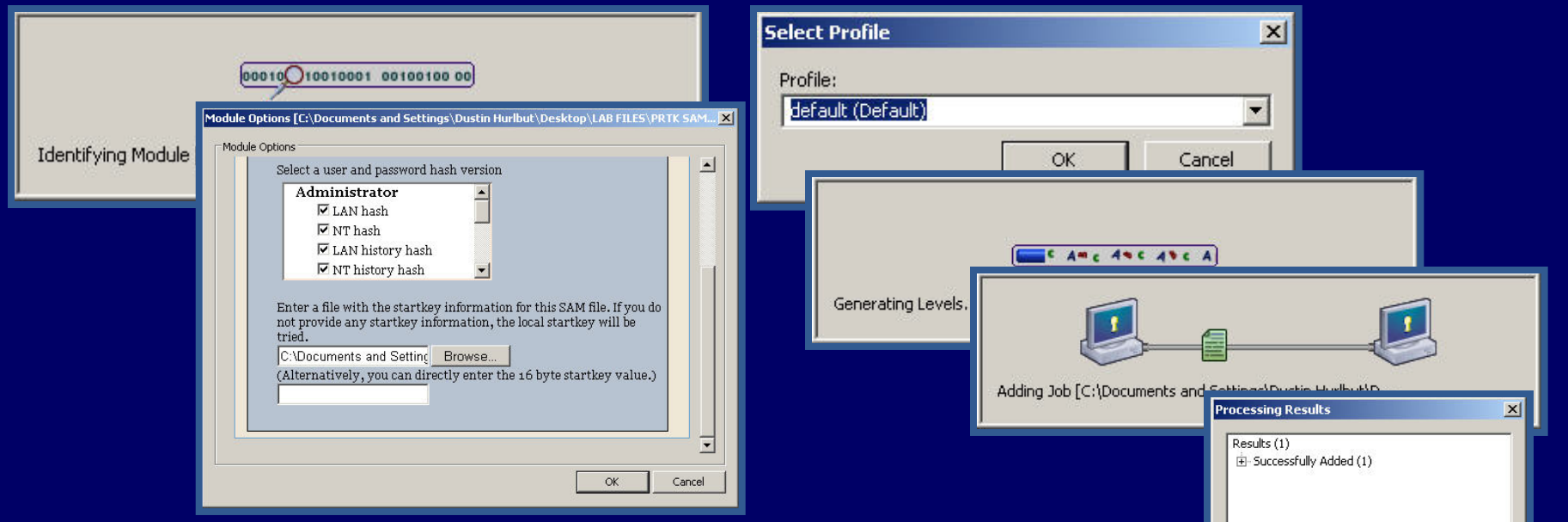
PRTK

Starting a Job – PRTK

- **Drop file into PRTK**



Decryption Steps

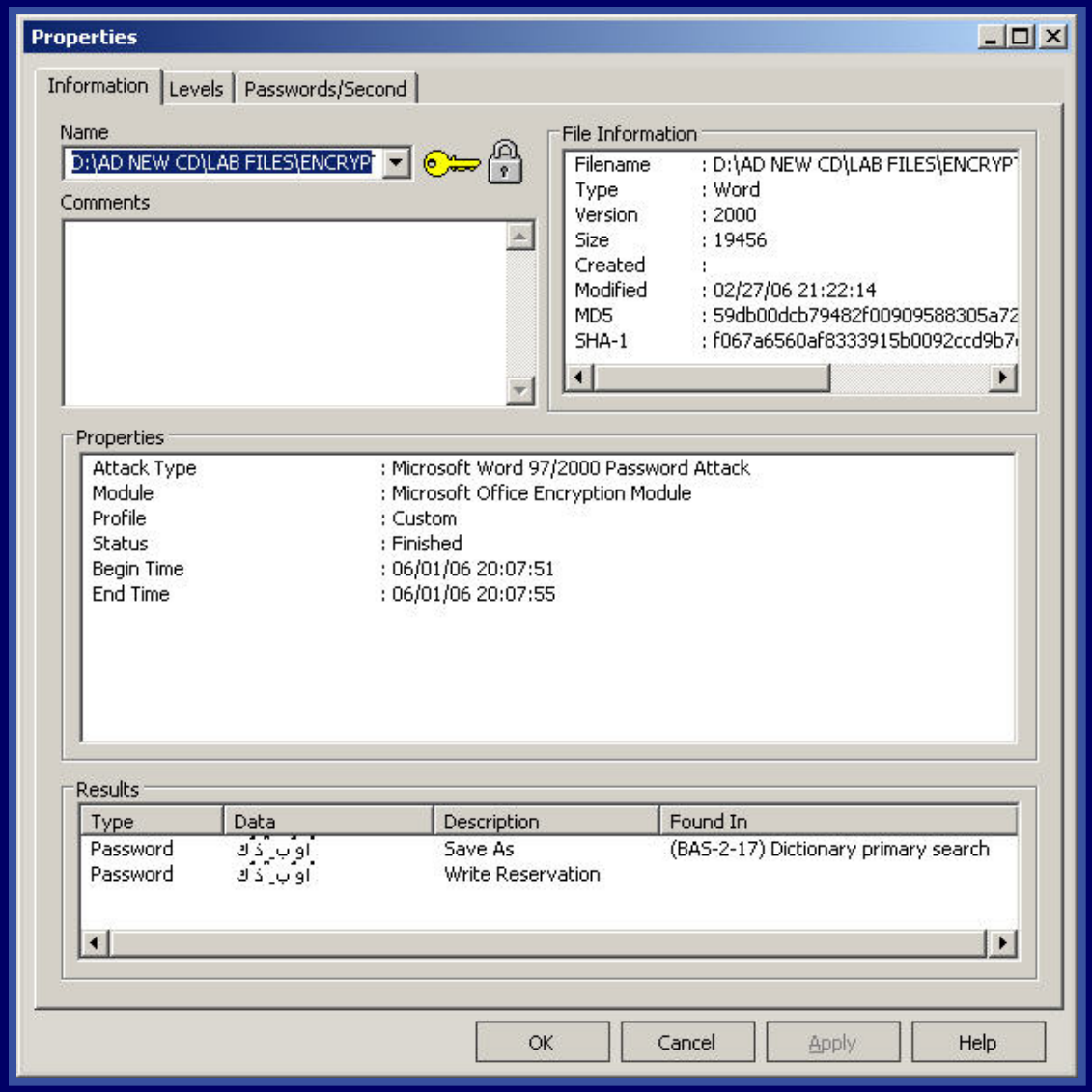


Filename	Attack Type		
C:\Documents and Settings\...	SAM user: VUSR_PHILLIP2000 [LAN history hash]		
C:\Documents and Settings\...	SAM user: VUSR_PHILLIP2000 [LAN hash]	Waiting On	
C:\Documents and Settings\...	SAM user: VUSR_PHILLIP2000 [NT hash]	Running	
C:\Documents and Settings\...	SAM user: VUSR_PHILLIP2000 [NT history hash]	Running	
C:\Documents and Settings\...	SAM user: Administrator [NT history hash]	Finished	giraffe
C:\Documents and Settings\...	SAM user: TsInternetUser [LAN hash]	Waiting On	
C:\Documents and Settings\...	SAM user: TsInternetUser [NT hash]	Running	
C:\Documents and Settings\...	SAM user: Administrator [NT hash]	Finished	giraffe

Properties – Information

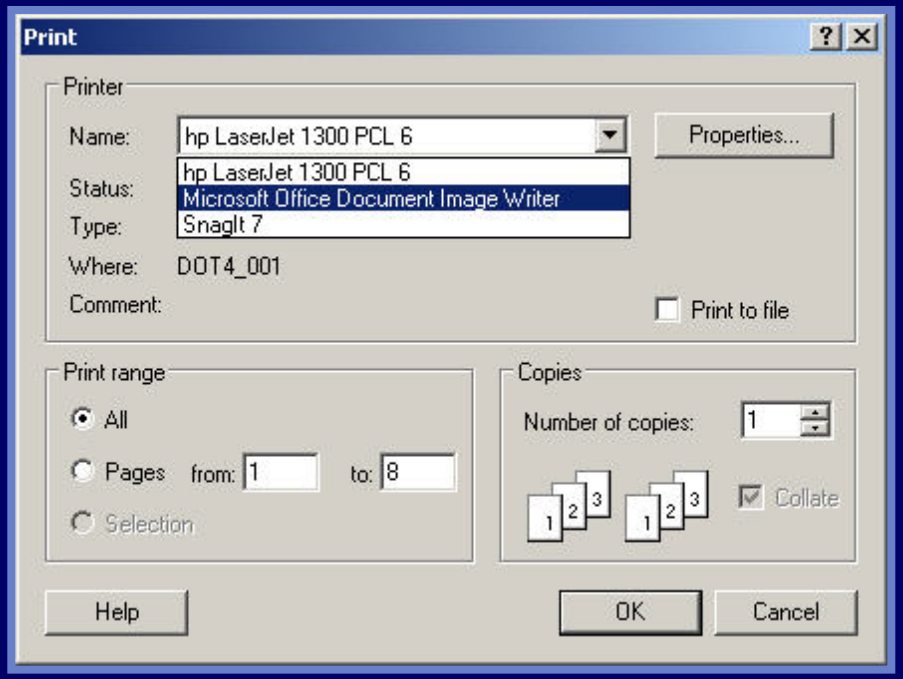
Basic File and Status Information

- File Name / Path
- Application Type
- Version
- Size
- Dates
- Hashes
- Attack Type
- Profile in use
- Status
- Time Begin / End



Documenting Results – PRTK

- **Written Reports**
- **Electronic Reports**



Documenting Results – PRTK

C:\Documents and Settings\Dustin Hurlbut\Desktop\Encrypted Files\Sagan\Was Einstein Right.doc

.....Commonly Registered Type: Microsoft Word Document

.....Identified Type: Word

.....Password gravity

PRTK REPORT 07/15/05

Description Save As

Found In Dictionary primary search (english-en-c.adf)

.....Size: 34816

.....File Version: 2000

.....Created: , Modified: 12/13/01 15:24:20

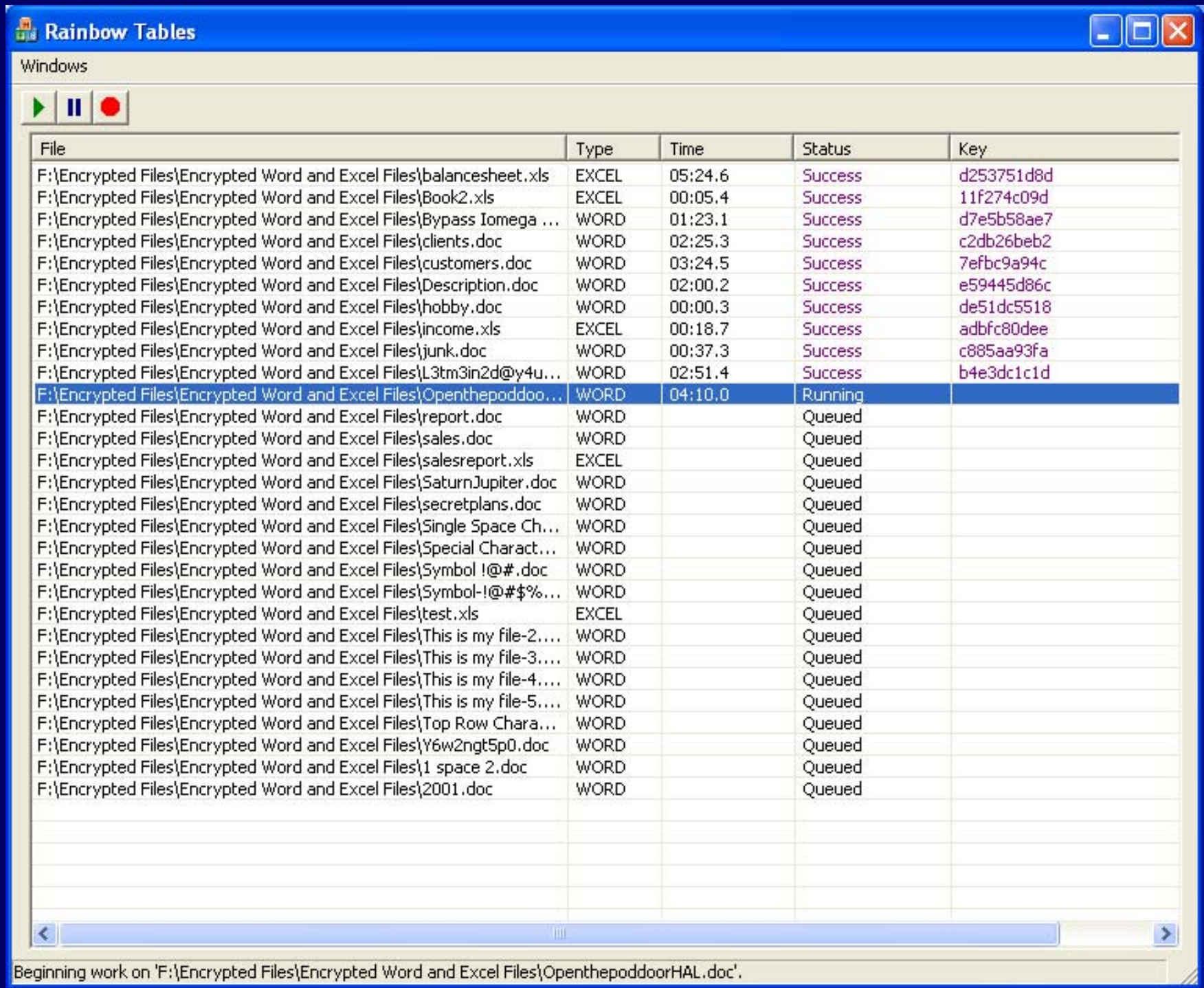
.....SHA: 6df9d2f067a411a8b72e5cbc81dbe32682b6ee44

.....MD5: b0cb1e80265b5f28fbeb97b2962d3b65

Rainbow Tables

Code Breaking Lookup Tables and Rainbow Table Technology

- Use pre-generated cipher text – file encryption key lookup tables to derive the key that will open 40-bit encrypted MS-Excel and MS-Word files.
- Recovery time is on the order of 1-5 minutes per file regardless of the password
- Able to provide the users login LAN and Windows NT passwords (i.e. attacking the hashes in the SAM file)


Rainbow Tables
Windows
File
Type
Time
Status
Key
F:\Encrypted Files\Encrypted Word and Excel Files\balancesheet.xls EXCEL 05:24.6 Success d253751d8d
F:\Encrypted Files\Encrypted Word and Excel Files\Book2.xls EXCEL 00:05.4 Success 11f274c09d
F:\Encrypted Files\Encrypted Word and Excel Files\Bypass Iomega ... WORD 01:23.1 Success d7e5b58ae7
F:\Encrypted Files\Encrypted Word and Excel Files\clients.doc WORD 02:25.3 Success c2db26beb2
F:\Encrypted Files\Encrypted Word and Excel Files\customers.doc WORD 03:24.5 Success 7efbc9a94c
F:\Encrypted Files\Encrypted Word and Excel Files\Description.doc WORD 02:00.2 Success e59445d86c
F:\Encrypted Files\Encrypted Word and Excel Files\hobby.doc WORD 00:00.3 Success de51dc5518
F:\Encrypted Files\Encrypted Word and Excel Files\income.xls EXCEL 00:18.7 Success adbfc80dee
F:\Encrypted Files\Encrypted Word and Excel Files\junk.doc WORD 00:37.3 Success c885aa93fa
F:\Encrypted Files\Encrypted Word and Excel Files\L3tm3in2d@y4u... WORD 02:51.4 Success b4e3dc1c1d
F:\Encrypted Files\Encrypted Word and Excel Files\Openthepoddoo... WORD 04:10.0 Running
F:\Encrypted Files\Encrypted Word and Excel Files\report.doc WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\sales.doc WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\salesreport.xls EXCEL Queued
F:\Encrypted Files\Encrypted Word and Excel Files\SaturnJupiter.doc WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\secretplans.doc WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\Single Space Ch... WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\Special Charact... WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\Symbol !@#.doc WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\Symbol-!@#$%... WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\test.xls EXCEL Queued
F:\Encrypted Files\Encrypted Word and Excel Files\This is my file-2.... WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\This is my file-3.... WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\This is my file-4.... WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\This is my file-5.... WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\Top Row Chara... WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\Y6w2ngt5p0.doc WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\1 space 2.doc WORD Queued
F:\Encrypted Files\Encrypted Word and Excel Files\2001.doc WORD Queued
Beginning work on 'F:\Encrypted Files\Encrypted Word and Excel Files\OpenthepoddoorHAL.doc'.

Attacking 128-bit Cryptosystems

- BestCrypt, WinZip (AES), WinRAR, PGP, DriveCrypt, etc.
- Keyspace is to large for lookup tables to be an option
- Only option is to “guess” the user’s password
- Biographical Profiling Options
  - NTUSER.DAT File
  - Web Crawling
  - FTK Export Word List
- The sweet spot for password lengths are 7-10 characters.
- The more resources that can be dedicated to the problem the higher probably of success

Other Tools

- John the Ripper
  - Primarily a user authentication password cracker (logon)
    - Unix, Windows LAN hash
- LC5 L0phtcrack - @stake = Symantec
  - NLA

Questions?

Code Breaking and Digital Forensics

FBI Supervisory Special Agent
Chris Beeson
Laboratory Director
Silicon Valley Regional Computer Forensic Laboratory
Menlo Park, CA
cbeeson@fbi.gov
www.rcfl.gov