



# AccessData Rainbow Tables

User Guide

May 2006



ACCESSDATA, ON YOUR RADAR

# TABLE OF CONTENTS

|   |          |
|---|----------|
| <b>ACCESSDATA RAINBOW TABLES.....</b>                       | <b>3</b> |
| <b>HOW ACCESSDATA RAINBOW TABLES WORK.....</b>              | <b>3</b> |
| <b>MS OFFICE.....</b>                                       | <b>3</b> |
| <b>ADOBE PDF.....</b>                                       | <b>3</b> |
| <b>WINDOWS LAN HASH (WINDOWS LOGIN PASSWORD).....</b>       | <b>5</b> |
| <b>USING RAINBOW TABLES WITH PRTK 6.2 AND DNA 3.2 .....</b> | <b>5</b> |
| <b>INSTALLATION.....</b>                                    | <b>5</b> |
| <b>OPERATION .....</b>                                      | <b>5</b> |
| <b>ATTACK SETTINGS .....</b>                                | <b>5</b> |
| <b>OPTIMIZING DISTRIBUTED NETWORK ATTACK.....</b>           | <b>7</b> |

## AccessData Rainbow Tables

Rainbow tables are a set of pre-computed lookup tables used to significantly accelerate a brute-force attack of several specific cryptosystems. In cryptography, a brute-force attack is a process of deriving a cryptographic key by trying every possible combination within a specific keyspace until the correct one is found. How quickly this key can be found depends on the size of the key space, and the computing resources applied.

A 40-bit cryptosystem has slightly more than one trillion keys ( $2^{40} = 1.099$  trillion). If a single computer can test 500,000 keys per second, this computer would need approximately 25 days to exhaust the key space. A rainbow table improves the efficiency of the brute force attack by having all possibilities precomputed and saved from the start. As a result, a single computer can break a 40-bit encrypted file in slightly more than a minute rather than in weeks.

Since 40-bit rainbow tables store up to one trillion entries, they are rather large. AccessData produces three types of rainbow tables:

- MS Office
- Adobe PDF
- Windows LAN hash

Each of our three Rainbow Tables is just under three (2.7) terabytes. The MS Office and Adobe PDF tables provide a key which decrypts and opens MS Office and Adobe PDF files. The Windows LAN hash provides the actual password needed to log in.

### How AccessData Rainbow Tables Work

Suppose you are trying to find a number (key) that will unlock a safe. The safe has numeric dials on it and each numeric dial can be set to 0–9 (similar to a child's bike lock). Since the key space is  $2^{40}$  there are a total of 12 dials. In order to open the safe, you need to set the dials to the correct number.

For example, if the key to open the safe were the number 254,365,476,587, you could sit down in front of the safe and start testing every possible number until you found the key that opens the safe. You might get it right on the first try, but more likely, it would take billions of attempts.

For a LAN hash, a computer can test hundreds of thousands of keys per second, testing all possible combinations in a few weeks. Suppose, however, you had a process that would allow you to quickly determine five

of twelve dials. In this case, the computer would need to try only seven dials to open the safe. All possible combinations of these seven dials can be completed in less than a minute.

## **MS Office**

MS Office 97 and 2000 derive a 40-bit encryption key from a user-supplied password. Our Rainbow Tables recover that 40-bit key in typically less than one minute. Once the key has been recovered, the document is decrypted.

**Note:** the Rainbow Tables recover only the decryption key. They do not find the original password. Even though MS Office XP and MS Office 2003 use as default a 40-bit encryption scheme, they have the capability to use 128-bit encryption keys. The Rainbow Tables are ineffective against attacking 128-bit encryption.

## **Adobe PDF**

Older PDF versions derive a 40-bit key from the user supplied password. Our Rainbow Tables recover that key, usually in less than a minute. Once the key has been recovered, the document can be decrypted. Again, the key, not the password, is recovered. Newer PDF versions use 128-bit keys and cannot be attacked with Rainbow Tables.

## Windows LAN Hash (Windows Login Password)

Windows LAN hash Rainbow Tables are a little different than MS Office or PDF Rainbow Tables. First, LAN hash tables recover passwords, not keys. Second, the number of possible LAN passwords is actually closer to 64 trillion ( $2^{46}$ ) so the AccessData LAN hash Rainbow Table is not actually a complete set of all possible LAN passwords. Rather, the LAN hash table represents the all possible passwords containing letters, numbers, and about 16 other symbols. This smaller set fits in about the same space as the Office and PDF tables.

The SAM file stores two different hashes of a user's password: the LAN manager hash, and the NT hash. LAN hash passwords are limited to 14 characters, which must be from the ASCII or extended ASCII character sets. (If the password is longer than 14 characters or has characters from outside those ranges, then only the NT hash is generated.) Unlike the NT hash, the LAN hash operates independently on the first seven characters on the left half and the last characters on the right half. DNA can attack the halves separately and, most importantly, that the number of possible LAN hashes is much smaller than the number of possible NT hashes. Small enough, in fact, that we can generate a substantial portion of all possible LAN hashes, and store them in a Rainbow Table. With these tables, you can look up a LAN hash and recover the corresponding password in a matter of seconds or minutes instead of days or weeks.

Both a SAM file and a system key file are needed to attack the Windows login password. FTK and FTK Imager are both useful tools for obtaining these registry files.

**Note:** the LAN hash Rainbow Table is effective only against Romantic language passwords. If the user logs into the computer using any Unicode password (Japanese, Korean, Chinese, etc.), a LAN hash value is never generated. The only way to break into these is using a DNA network to perform a traditional MS Windows Login password guessing attack.

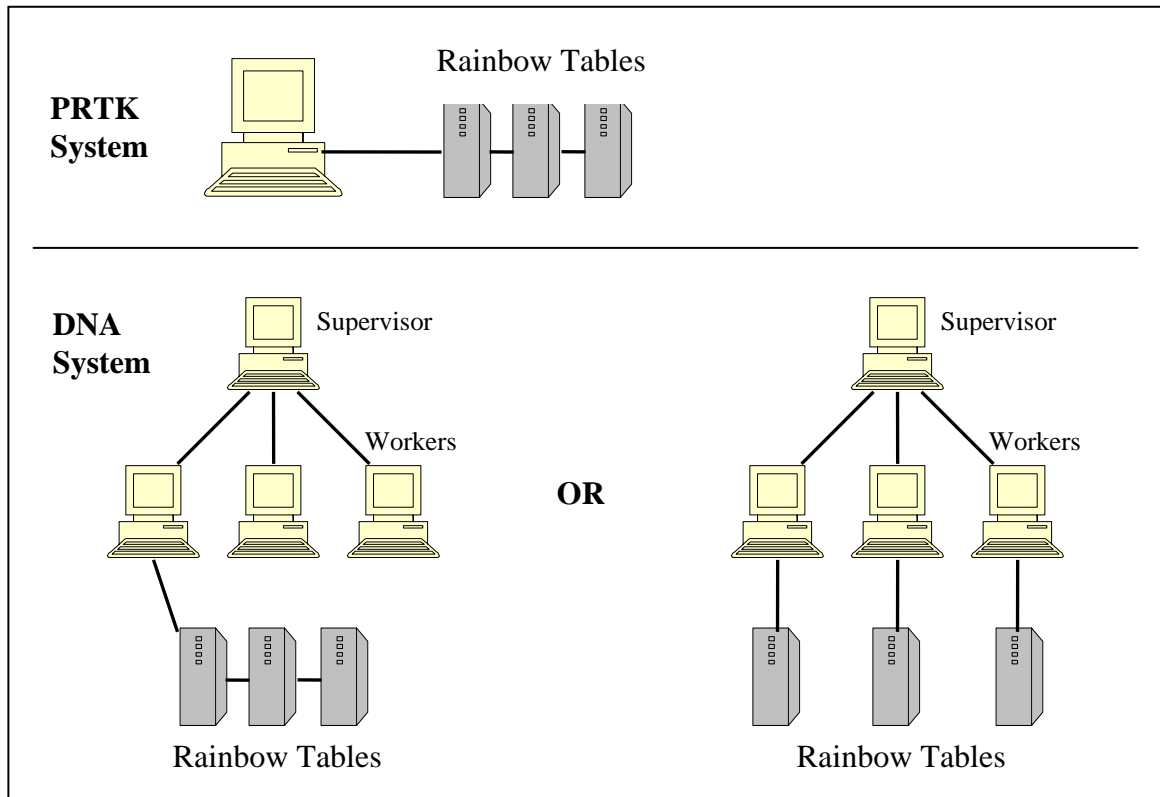
## Using Rainbow Tables with PRTK 6.2 and DNA 3.2

Each Rainbow Table set is independent of the others and may be used by itself or in conjunction with PRTK 6.2 or DNA 3.2.

### Installation

For PRTK 6.2, the Rainbow Table drives must be connected to the computer with PRTK installed. When using DNA 3.2, the rainbow tables must be connected to one or more of the DNA workers. The hardware connections for a single set of Rainbow Tables are illustrated in the figure

below. Multiple sets of rainbow tables can be connected in a similar manner. As long as DNA workers can see the rainbow tables on a drive letter, they will automatically configure themselves to work with the tables. DNA workers look for Rainbow Tables only on local drives, however, they will not search mapped network drives.



## Operation

When using PRTK, select **Analyze** from the main application menu, and then Select **Files**. Specific files are submitted for a Rainbow Table attack depending on which set of tables are connected to the system (MS Office, PDF, or LAN Hash). Files may also be submitted by dragging and dropping them onto PRTK, creating new jobs. Once a job has been identified, the job wizard will display requesting which type of attack should be performed.

When using DNA, select **Files** from the supervisor application menu, then **Add Job**. New jobs can also be created by dragging and dropping them onto DNA. A job wizard will allow selection of the type of attack to perform.

## Attack Settings

The following table describes the proper attack settings for each file type.

Any profile can be used for each of these attack types.

| File Type | Attack Settings  |
|-----------|--|
| MS Office | Uncheck all boxes except “Decryption Key Attack”   |
| PDF       | Uncheck all boxes except “PDF User Key Attack”   |
| LAN Hash  | Check only boxes that choose a LAN Hash attack for the desired user account. Do not check any options for NT Type attacks. |

PRTK and DNA will generate the appropriate levels, and then add the job to the main display window. Both applications will use the correct module and use the installed Rainbow Tables for decryption.

## Optimizing Distributed Network Attack

Jobs submitted to DNA for decryption are processed normally in the order of submission. Due to this design, jobs submitted for Rainbow Table attacks have to wait until the workers with the Rainbow Tables attached are available.

DNA allows the creation of specialized groups in which one or more workers can be associated. By creating a group containing the workers with the Rainbow Table set attached, jobs can be submitted directly to allow an immediate attack. This allows other types of jobs to be submitted to non-rainbow table workers, keeping the rainbow table workers available for immediate access.