

TABLE OF CONTENTS

ACCESSDATA RAINBOW TABLES	3
HOW ACCESSDATA RAINBOW TABLES WORK.....	3
MS OFFICE	4
ADOBE PDF	4
WINDOWS LAN HASH (WINDOWS LOGIN PASSWORD)	5
USING RAINBOW TABLES WITH PRTK 6.2 AND DNA 3.2	5
INSTALLATION	5
OPERATION	6
ATTACK SETTINGS	6
OPTIMIZING DISTRIBUTED NETWORK ATTACK	7

AccessData Rainbow Tables

Rainbow tables are pre-computed, brute-force attacks. In cryptography, a brute-force attack is an attempt to recover a cryptographic key or password by trying every possible combination until the correct one is found. How quickly this can be done depends on the size of the key, and the computing resources applied.

A system set at 40-bit encryption has one trillion keys available. A brute-force attack of 500,000 keys per second would take approximately 25 days to exhaust the key space combinations using a single 3 Ghz Pentium 4 computer. With a Rainbow Table, you can decrypt 40-bit encrypted files in seconds or minutes rather than days or weeks.

Since rainbow tables store the result from every possible key test, they are typically very large. AccessData has 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 first two tables provide a key with which to open an encrypted file. The third provides the actual password.

How AccessData Rainbow Tables Work

Suppose you are trying to find a key that will unlock a safe. The safe key is a number between 1 and 1 trillion. In order to unlock the safe, you need to type in the correct password to be converted to the safe's key.

For example, if you were to find a safe with the number 88888 for a key, you could sit down and guess various passwords until you find one that equals 88888 and opens the safe. You might get it right on the first try, but more likely, it would take over a trillion or more tries.

Since the password to number conversion always works the same, any safe with the number 88888 on it can be opened with the password once you guessed it.

A computer can try a trillion passwords in a relatively short amount of time, usually a few weeks. But that is still slower than what it could do with AccessData Rainbow Tables.

Suppose you had a hard drive big enough to hold a trillion passwords. You could put the computer to work generating and testing each possible key from a password and in about a month or two you could produce a list of password matches for every possible safe number! If you had a hard drive big enough to store this list (and it would take about ten terabytes), you could use it to

immediately look up the password to open any safe. All you would have to do is find the key number for the safe, and then look it up in the table to find the matching password. This list is called a rainbow table.

Buying and selling ten-terabyte hard drives is difficult and expensive. AccessData stores partial passwords on three-terabyte drives to make our rainbow tables more economical. When you want to break open a safe, you look up the “partial password” in the table. The partial password doesn't open the safe, but it makes it possible for the computer to find the complete password very quickly.

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 can be decrypted.

Note: the rainbow tables recover only the decryption key. They do not find the original password. MS Office XP and 2003 have the capability to use 128-bit encryption keys, but the old 40-bit key scheme is used by default.

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)

These rainbow tables are a little different than the others. First, they recover passwords, not keys. Second, the number of possible LAN passwords is much more than a trillion (the approximate size of a 40-bit key space), so it is not practical to generate a complete set of LAN rainbow tables. However, if we restrict the set of characters in the passwords to letters, numbers, and about 16 other symbols, then the rainbow tables covering these passwords fit 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, 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 for this type of attack. FTK Imager is a useful tool for obtaining both of these registry files.

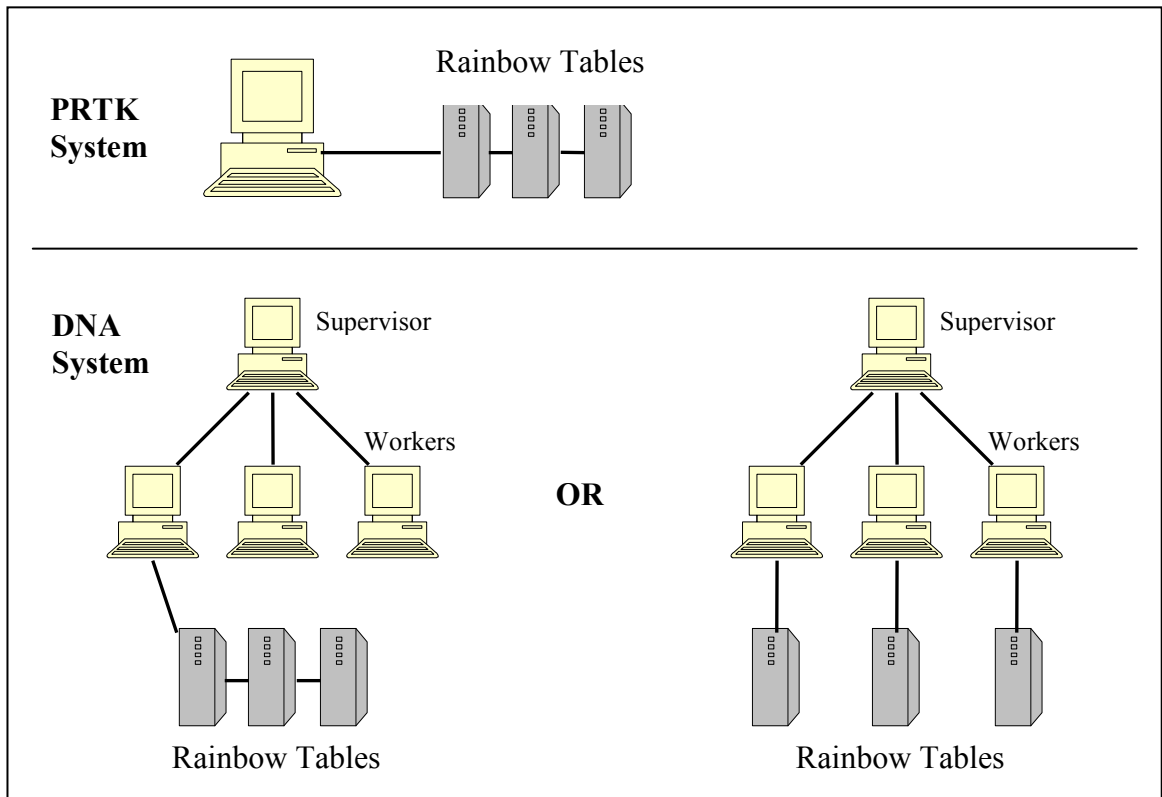
Note: the LAN hash rainbow table is effective only against Romantic language passwords. If the user logs into the computer using any Unicode password (Japanese, Korean, Chinese, etc.), a LAN hash value is never generated. The only way to break into these is using a traditional Windows Login password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

Using Rainbow Tables with PRTK 6.2 and DNA 3.2

Each Rainbow Tables set is independent of the others and may be used with PRTK or DNA alone, or connected to the system.

Installation

For use with PRTK 6.2, the Rainbow Table drives must be connected to the computer where PRTK is installed. For use with DNA 3.2, the drives may be connected to a single worker or to a set of workers. The hardware connections for a single set of Rainbow Tables are illustrated in the figure below. Multiple sets can be connected in a similar manner. The operating system should recognize the new hardware and assign drive letters automatically.



Operation

When using PRTK, select **Analyze** from the main application menu, 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.