User Manual for 2-Dimensional Key (2D Key) Input Method and System

Version 2.0 as at 08Sep08

2D Key PW5 2.0 Free Edition

Requirement: Pentium D 2.80 GHz or better, 512 MB RAM or better, Windows XP and Microsoft .NET Framework Version 1.1 Redistributable Package (23698KB) or better from http://www.microsoft.com.

Procedure

1) Double click the icon of "2D_Key.exe". A window as in Figure 1 will be shown.

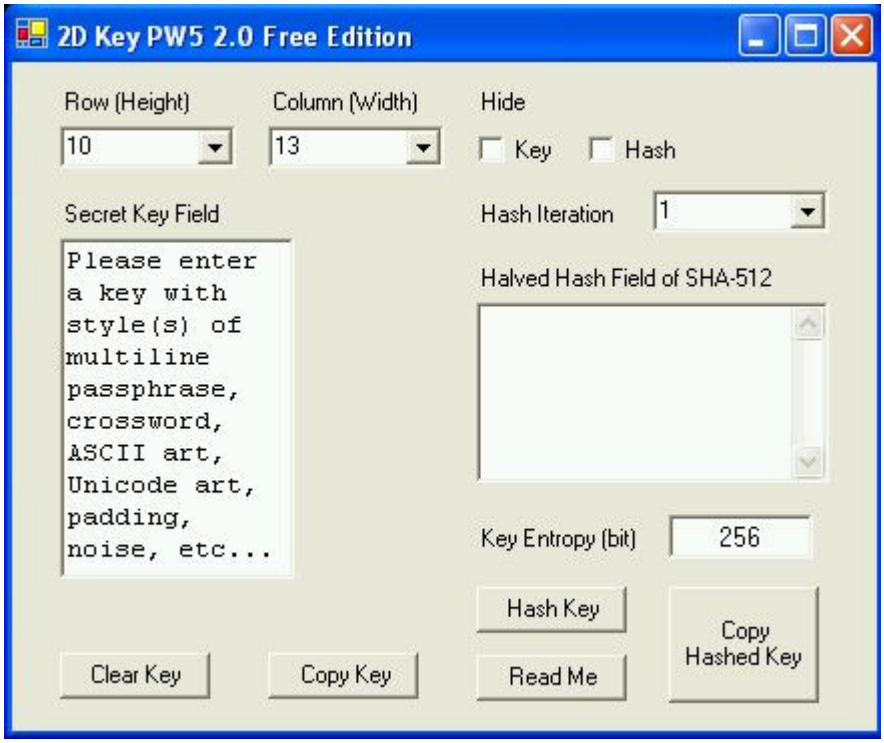

Fig. 1 Starting screen of 2-dimensional key input method and system

2) The textbox of "Secret Key Field" can have inputs of printable ASCII symbols and graphic Unicode symbols depending on the support of end user's application. For printable ASCII symbol, keyboard can be used. For graphic Unicode symbols, enter a symbol using any input method via keyboard, mouse, etc. For example, holding the button of "Alt", enter the Unicode in decimal value, and release the button of "Alt" to input a graphic Unicode symbol. Try "Alt" and "0165" for "¥". Graphic Unicode symbols may occupy one or two locations in the column dimension.

3) There are many possible styles of keys for this input method: **Multiline passphrase**, **crossword**, **ASCII art/graphics**, **Unicode art/graphics**, **padding**, **noise**, etc.

4) The textbox of “Key Entropy (bit)” shows the effective key size in bit of key, up to a maximum of 256 bits, in the textbox of “Secret key Field”. It is 6.57 bits per ASCII symbol ($\log_2 95$) and 16 bit per Unicode symbol ($\min(16, \log_2 98884)$).

5) To avoid the automatic wrapping of symbols that causes the unwanted alignment, enter ASCII and/or Unicode symbols after checking the checkbox of “Hide Key”.

6) For key style of multiline passphrase, padding is needed for easy recognition of the starting location of each word in the passphrase. First, click the button of “Clear Key”. Second, check the checkboxes of “Hide Key” and “Hide Hash” to hide the key and hash respectively. Third, set the row to the number of words in the passphrase. Fourth, set the column to the number of character of the longest word in the passphrase.

Fifth, enter the key of passphrase into the textbox of “Secret Key Field”. One word is for one line. For word shorter than the longest word, pad it with a padding character until the length of the longest word. Once finish, if there is no threat of shoulder-surfing attack from anyone to be able to view the displaying screen, input key may be view to confirm the correctness by unchecking the checkbox of “Hide Key”.

Sixth, for different unique slave keys from a master key at the Secret Key Field, select the number of hash iteration, from 1 to 5. For more slave keys, please switch to higher version of 2D Key. Seventh, click the button of “Hash Key” to get a halved SHA-512 hash of the input key. To view the hash, uncheck the checkbox of “Hide Hash”.

Figure 2 displays an example of 4 x 5 multiline passphrase with padding character “*”:

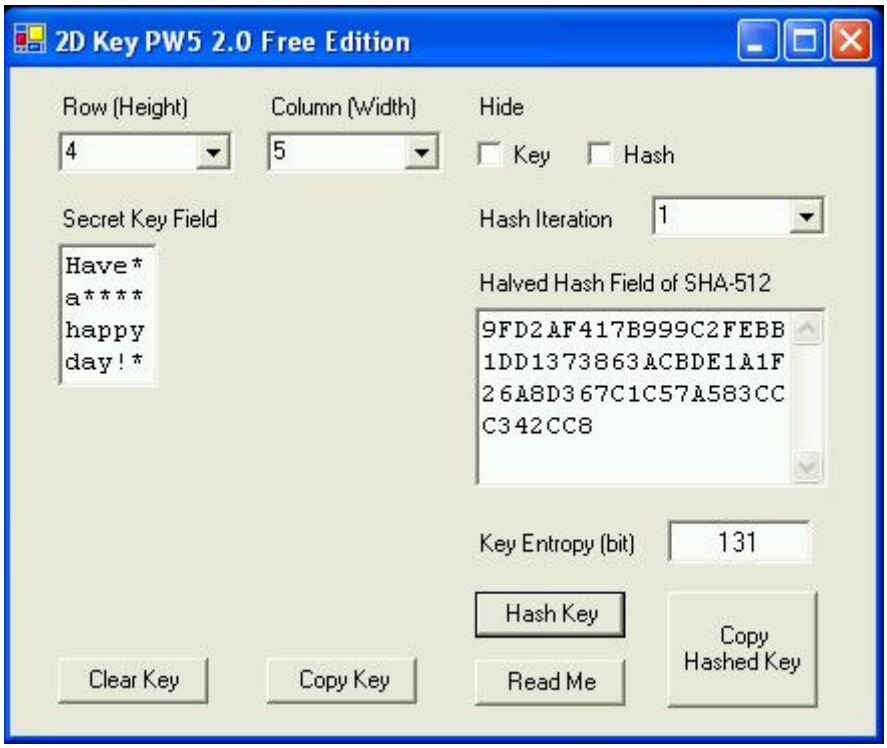

Fig. 2 Key style of multiline passphrase with padding character “*”

The number of ASCII characters is 20 (= 4 x 5), and hence the nominal key size is 160 bits (= 8 x 20). Meanwhile, the effective key size is 131 bits (= 20 x $\log_2 95$).

For the one-key encryption or symmetric encryption of 128-bit AES (Advanced Encryption Standard), 16 ASCII characters can give the nominal key size of 128 bits (= 8 x 16). However, this is not enough for real security strength at 128 bits. Effective key size has to be referred instead of nominal key size. Hence, security strength at 128 bits is achieved when the effective key size is more than 128 bits.

To insert to the prompt of key / password space, click either the button of "Copy Key" or "Copy Hashed Key" for the master key at the Secret Key Field or slave key at the Hash Field, respectively. "Copy Key" button copies the ASCII characters of the input master key. "Copy Hashed Key" button copies the halved 512-bit hash (i.e. slave key) of the input master key. As an information, SHA-512 is used here. Then, click the key space of the prompt of any software application. Press "Ctrl + V" using the keyboard. Now, either the input master key or the halved SHA-512 hashed key (i.e. slave key) will be pasted. Press "Enter" to gain authorization access. **Lastly**, **press** the button of "**Clear Key**" to clear the input master key or hashed key (i.e. slave key) in the clipboard of the computer memory.

7) For key style of crossword, background character is needed. Figure 3 shows a 5 x 6 crossword with background character of "*". Alike multiline passphrase, either input master key or hashed key (i.e. slave key) can be used. This example can be used as a key for AES-192.

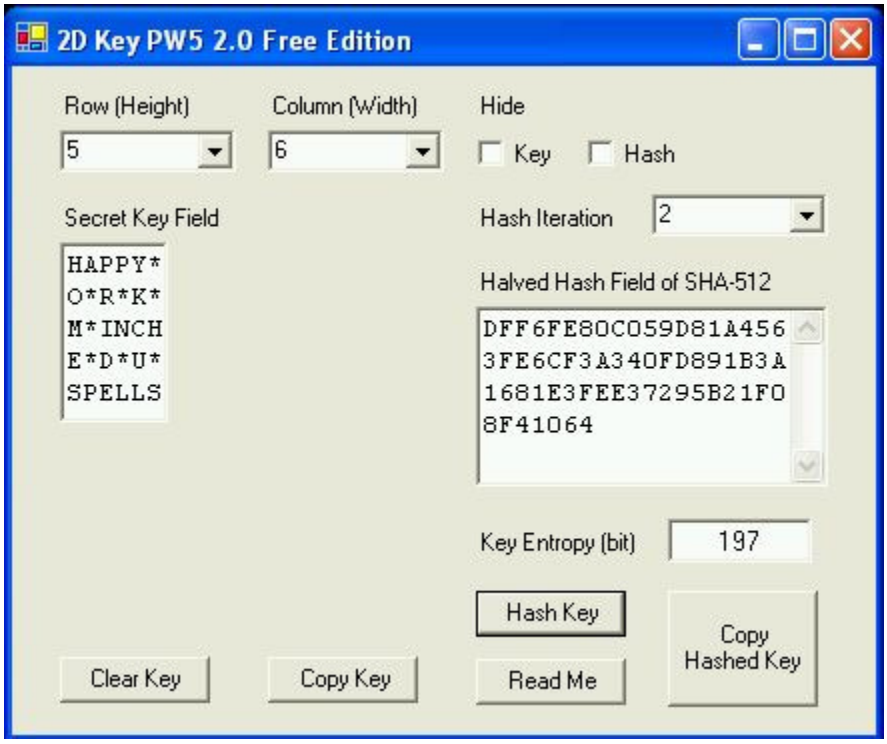

Fig. 3 Key style of crossword with background character of "*"

8) For key style of ASCII art/graphics, Figure 4 illustrates this type of example using a 2-dimensional key space of 7 x 6. The drawn graphics is the Han character of "engineering" in Chinese language. Alike other key styles, either input master key or hashed key (i.e. slave key) can be used. This example can be used as a key for AES-256.

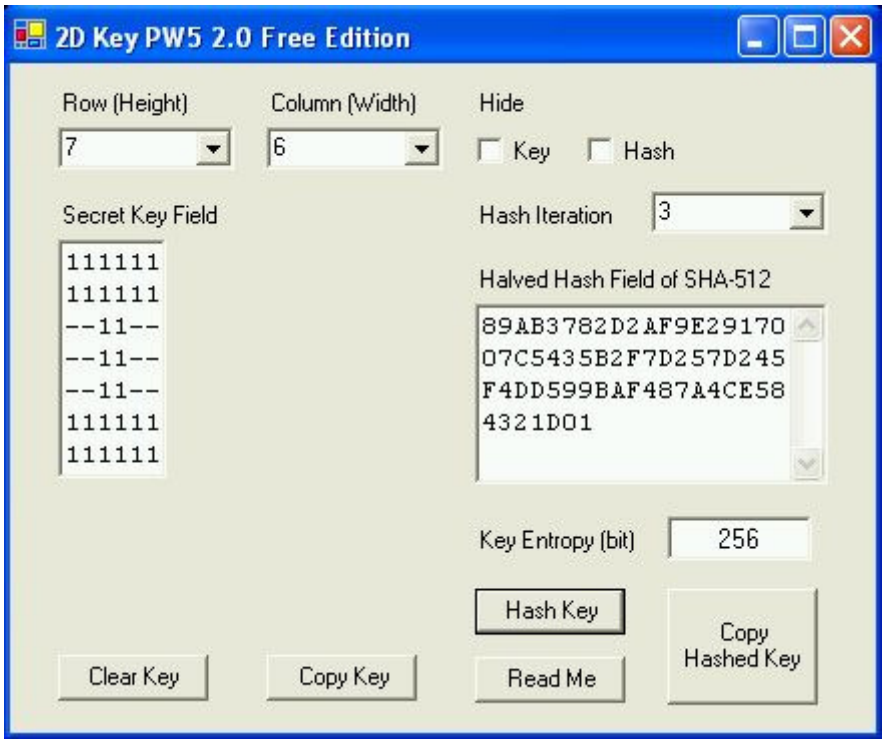

Fig. 4 Key style of ASCII art/graphics

9) For key style of Unicode art/graphics, Figure 5 illustrates this type of example using a 2-dimensional key space of 4 x 5. The drawn graphics is the Han character of "engineering" in Chinese language using the Unicode symbols of "¥" (Alt + 0165) and "©" (Alt + 0169). Alike other key styles, either input master key or hashed key (i.e. slave key) can be used.

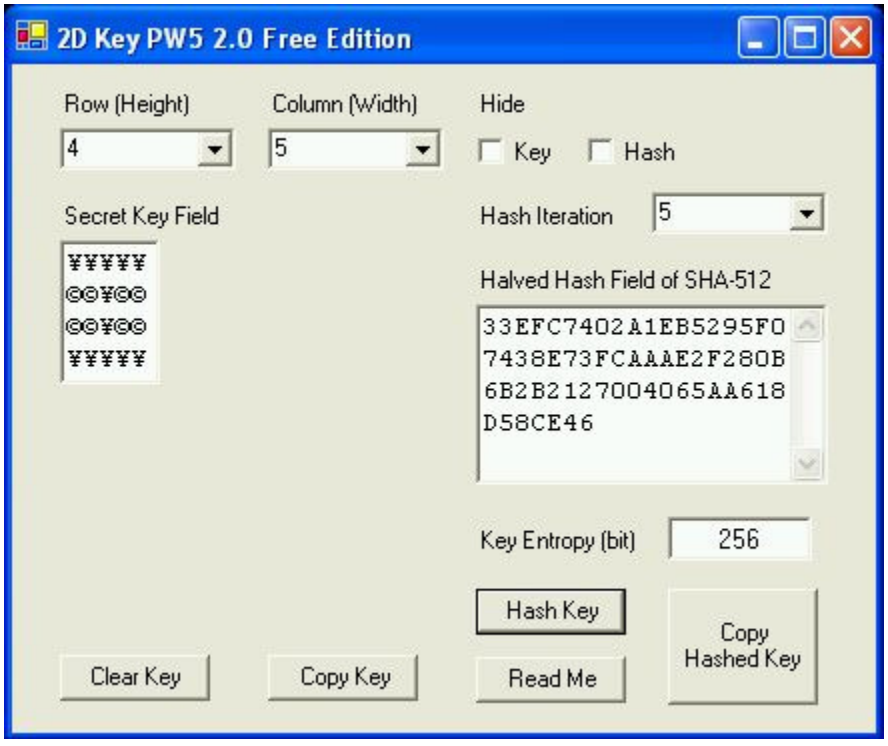

Fig. 5 Key style of Unicode art/graphics

10) A mixture of various key styles is also encouraged. Among them, adding semantic noise(s) is the easiest. This example can be observed as in Figure 2 using the exclamation mark "!". Using semantic noise, the effective key size can be adjusted by 6 or 7 bits per ASCII symbol and 16 bits per Unicode symbol.

11) To know the more information of this software about its IPR (Intellectual Property Rights) and contact, please click the button of "Read Me".

*** The End ***