

SyferLock Technology Corporation™

# GridAdvanced™ Security Analysis



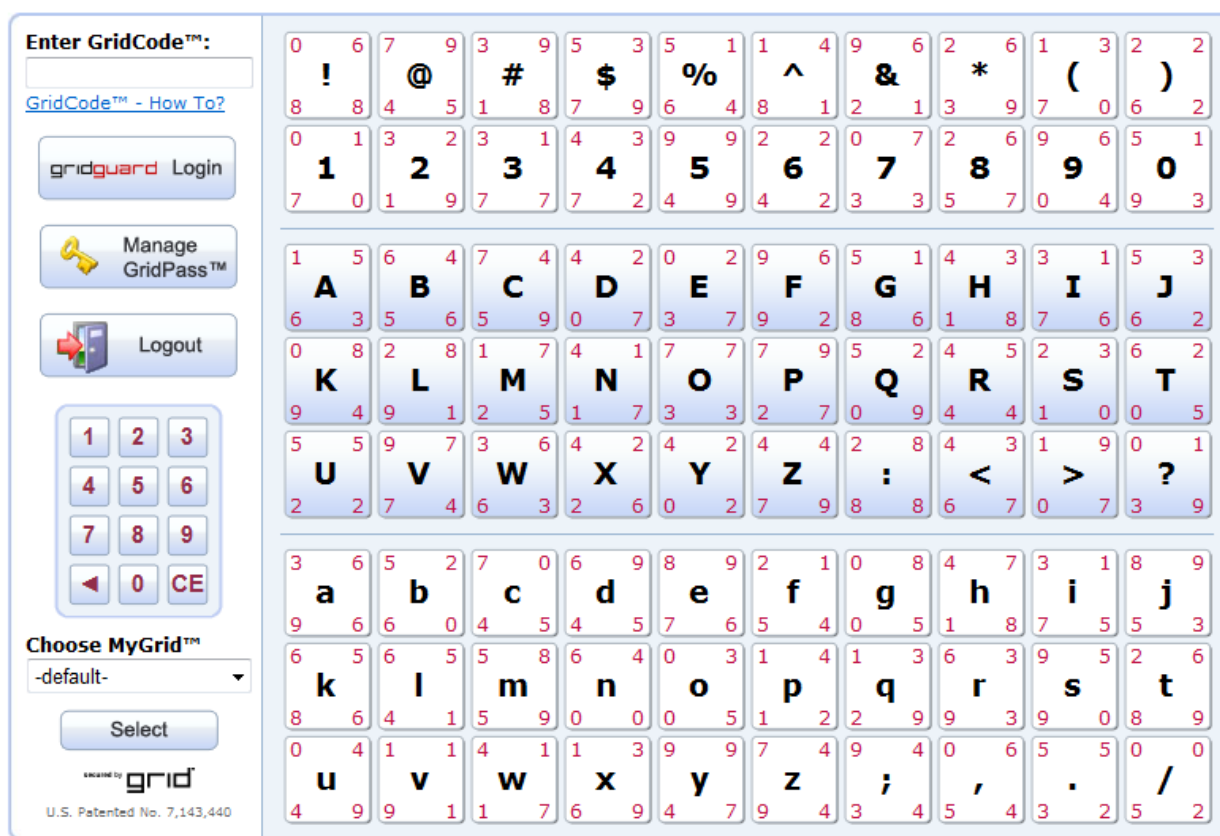
# GridAdvanced™ Authentication System

## Security Analysis

### 1 Introduction

Grid Data Security's GridAdvanced authentication scheme is a system that provides the security of a one-time password without the inconvenience or cost of deploying a "hard" or "something you know" second factor. The GridAdvanced authentication scheme is as easy to use as a standard password authentication mechanism, yet extremely secure in insecure, open, and compromised environments where attackers have the ability to observe authentications or have complete control over the computer.

GridAdvanced works by providing a user with a randomly generated Grid that contains password characters and GridCode™ digits. A user authenticates with GridAdvanced by typing in the corresponding GridCode digits associated with the password characters of their GridPass™. The GridCode digits are determined by referencing the password characters in the Grid at the proper corner of each GridCell. Figure 1 shows an example of the scheme's user interface. Each GridCell has four GridCode digits and a single GridPass character associated with the GridCell. Figure 2 shows a single GridCell for the GridPass character 'A'.



The interface is divided into two main sections. The left section contains a login form with the following elements:

- Enter GridCode™:** A text input field.
- [GridCode™ - How To?](#) link.
- gridguard Login** button.
- Manage GridPass™** button with a key icon.
- Logout** button with a red arrow icon.
- A numeric keypad with digits 1-9, 0, and a CE button.
- Choose MyGrid™** dropdown menu set to "-default-".
- Select** button.
- Logo for "grid" with "U.S. Patented No. 7,143,440" below it.

The right section displays a large grid of 100 cells (10 rows by 10 columns). Each cell contains a single GridPass character and four GridCode digits at the corners. The characters are arranged in rows: Row 1: !, @, #, \$, %, ^, &, \*, (, ), ;. Row 2: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0. Row 3: A, B, C, D, E, F, G, H, I, J. Row 4: K, L, M, N, O, P, Q, R, S, T. Row 5: U, V, W, X, Y, Z, :, <, >, ?. Row 6: a, b, c, d, e, f, g, h, i, j. Row 7: k, l, m, n, o, p, q, r, s, t. Row 8: u, v, w, x, y, z, ;, , ., /. Row 9: (empty), (empty), (empty), (empty), (empty), (empty), (empty), (empty), (empty), (empty). Row 10: (empty), (empty), (empty), (empty), (empty), (empty), (empty), (empty), (empty), (empty).

Figure 1: The GridAdvanced Authentication Interface

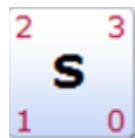


Figure 2: GridCell

To authenticate with the system using the Grid in Figure 1, a user must have a password and a corner (GridPass) registered with the system. For example, the password “PaSSw0rd” and the top right corner results in a GridCode of “96331139”. The system also allows for DecoyDigits™. DecoyDigits are fake GridCode digits that are placed in between real GridCode digits to make it even more difficult for an attacker to determine the GridPass after observing the authentication process. Going back to the example, “9623311379” (DecoyDigits are underlined) would be a valid GridCode if the system is configured to allow one DecoyDigit for every three GridCode digits.

By translating from GridPass characters to GridCode digits, a user in a hostile environment does not reveal their GridPass to someone monitoring what they type. This type of an attack, along with others, are compared side-by-side to a standard password authentication system in the rest of this paper. Section 2 describes the attack scenarios that are considered. Section 3 compares how secure the system is for each attack scenario when DecoyDigits are not used. Section 4 expands upon the previous section by including the use of DecoyDigits. Finally, Section 5 provides some concluding remarks on the subject.

## 1.1 Terms and Notation

Before defining the attack scenarios that are considered in this paper, terms and notations are defined. Whenever possible the terms and notation match those most commonly used in the field.

**Definition 1 (GridCell)** *A polygon (usually a square or rectangle) consisting of a single GridPass character in the middle and corresponding GridCode Digits for each corner of the cell. See Figure 2 for an example.*

**Definition 2 (Grid)** *A set of Grid Cells sent to the user as a challenge for which the user must correctly respond with an appropriate GridCode™ to be authenticated with the system. See Figure 1 for an example.*

**Definition 3 (GridCode™)** *The response to the Grid challenge. A GridCode contains the digits from the Grid Cells that correspond to the user's GridPass. The GridCode may also contain DecoyDigits.*

**Definition 4 (GridCode digit)** *A single character in the GridCode. While usually decimal digits, the set could contain any characters.*

**Definition 5 (GridPass™)** *A standard password consisting of characters from the set of possible password characters and an associated corner on the Grid (or another security modifier allowed by the system).*

**Definition 6 (DecoyDigit™)** *A single digit that is inserted into the GridCode. The digit is from the set of possible GridCode Digits.*

There are a number of parameters that change how secure an authentication system is. These parameters are determined by the institution's security policy that is using the authentication scheme. For the purposes of this paper the following parameters and variables representing them are defined.

**Definition 7 (Password Character Set)** *Let  $P$  represent the cardinality of the set of possible password characters. For the purposes of this paper we will define this set to be all uppercase and lowercase characters, decimal digits, and eighteen of the most common special characters (such as + - # .). Therefore,  $P = 80$ .*

**Definition 8 (Password Length)** *Let  $N$  represent the length of a password. For the purposes of this paper we will let  $N=8$ .*

**Definition 9 (GridCode Character Set)** *Let  $\Pi$  represent the cardinality of the set of possible GridCode characters. For the purposes of this paper we will let  $\Pi=10$ , or the decimal digits.*

**Definition 10 (Number of Unsuccessful Authentications)** *Let  $k$  represent the number of unsuccessful authentications for a single user before that user is locked out of the system. In most system, as in this paper, this number is  $k=3$ .*

## 2 Attack Scenarios

There are four basic types of attacks against the GridAdvanced authentication scheme. These attacks do not rely on the specific details of the implementation of GridAdvanced, but rather focus only on the method used to authenticate. Therefore, these attacks are generic and do not consider specific attacks such as buffer overflows.

The attack scenarios also give the attacker much more freedom than a typical attacker would have. This freedom is given to the attacker in the form of a set of assumptions made about the system.

The first assumption is that there is only one user in the system to attack. Therefore, the attacker never needs to worry about disambiguating between users when observing valid authentications or when trying to authenticate with the system. Second, the attacker has unbounded computational power. For example, the attacker can solve NP problems quickly. While it is highly unlikely that an attacker will actually have this kind of computational power, the purpose of this document is to compare the relative strength of GridAdvanced to a standard password authentication scheme. Third, it is assumed that the attacker knows the inner workings of the system. This means the attacker knows that the Grids are randomly constructed, how many DecoyDigits are allowed (if any), and the possible GridPass characters and GridCode digits. Finally, it is assumed that a user always enters a valid GridCode or password. This is a safe assumption to make because if the user does not correctly authenticate with the system, the attacker will know by the observed response from the server.

### 2.1 Random Guess of the Password

For this type of attack, the attacker attempts to guess the correct password in  $k=3$  attempts. An attacker is considered successful if the number of possible passwords is less than or equal to  $k$ . It is also assumed that the attacker knows the length of the password in advance.

For the standard password authentication mechanism, the attacker tries to guess the user's password. In the GridAdvanced scheme the user is trying to guess the user's GridPass, but must enter the corresponding GridCode to test the guess.

This type of attack is often described as a dictionary attack. Instead of the attacker searching through all possible passwords, the attacker searches only through a dictionary of possible words. The attacker hopes that a user's password will appear in the dictionary and therefore can be discovered more easily than searching through all possible passwords. For the purposes of this paper the dictionary attack will not be evaluated.

### 2.2 Random Guess of a Valid GridCode

For this type of attack, the attacker is simply trying to authenticate with GridAdvanced. For the standard password authentication mechanism, the only way an attacker can authenticate with the system is by discovering the user's password. Therefore, there is no analogy for the standard password authentication scheme.

For GridAdvanced, the attacker need only guess a correct GridCode for the corresponding Grid.<sup>1</sup> Again, it is assumed that the attacker knows the length of the password in advance.

### 2.3 Observing an Authentication

In this scenario the attacker is able to observe a single valid authentication. From the knowledge of this valid authentication, the attacker must guess the correct password from the set of possible passwords that can be constructed after the observation.

For a standard password authentication scheme observing a valid authentication entails the attacker recording the password that is entered. This is traditionally done by either observing the keys that were pressed on the keyboard, or by key logging software that records the keystrokes of the user. Once this password has been recorded, the account is compromised and the attacker can gain access.

---

<sup>1</sup>It is important to note that with GridAdvanced, a single authentication does not guarantee future authentications; whereas, with the standard password scheme future authentications are guaranteed. Once an attacker authenticates with the scheme, they have discovered the password and can continue to authenticate.

For GridAdvanced, observing a valid authentication requires recording the GridCode that was entered and also the Grid that was presented. If the attacker is only able to record the GridCode this will not help in reducing the set of possible passwords. The attacker must be able to record both the screen and the GridCode that is entered. It is this attack scenario which highlights the strength of GridAdvanced versus a standard password authentication scheme: the ability to have an attacker observe an authentication and still not know the user's GridPass.

### 3 Probability of Success Without DecoyDigits

Before discussing the success of an attacker against the complete GridAdvanced scheme which uses DecoyDigits, it is helpful to consider GridAdvanced without DecoyDigits. This is beneficial because it gives a very strong “apples-to-apples” comparison between the GridAdvanced and a standard password authentication scheme. It is also beneficial for those administrators who choose to not let their users add DecoyDigits to the GridCode.

#### 3.1 Random Guess of the Password

A random guess of the GridPass is different than a random guess of the password in a standard authentication scheme. In a standard authentication scheme the number of possible passwords is the set of password characters raised to the length of the password. For GridAdvanced, this value is multiplied by the number of corners in a GridCell. Therefore, assuming the attacker knows the length of the password is  $N=8$ , the number of possible passwords for the standard authentication scheme is  $P^N$ ; whereas with GridAdvanced it is  $P^N \times 4$ . Allowing the attacker to make  $k = 3$  guesses for a standard authentication scheme, the probability of the attacker guessing the password is

$$\frac{k}{P^N} = \frac{3}{80^8} = \frac{1}{559,240,533,333,333}$$

For GridAdvanced the probability shrinks to

$$\frac{k}{P^N \times 4} = \frac{3}{80^8 \times 4} = \frac{1}{2,236,962,133,333,333}$$

#### 3.2 Random Guess of a Valid GridCode

A random guess of a proper authentication is exactly the same as guessing the password in the standard password authentication scheme. However, for GridAdvanced this means guessing only a valid GridCode. The probability of guessing the correct password for the standard authentication scheme is the same as above; whereas, the probability of guessing a correct GridCode is

$$\frac{1}{H^N} = \frac{1}{10^8} = \frac{1}{100,000,000}$$

Allowing the attacker to make  $k = 3$  guesses of the GridCode does not help the attacker like it does for guessing the password. This is because the Grid changes with each authentication attempt. Therefore, an invalid GridCode for one Grid might be a valid GridCode for the next Grid. In terms of probability, this can be thought of as replacement after selection. Therefore, allowing the attacker to make  $k$  guesses of the GridCode keeps the probability the same as Equation (3). However, as  $k$  increases, the security of the standard password authentication mechanism decreases.

### 3.3 Observing an Authentication

In the standard password authentication mechanism, after observing a single authentication the attacker knows the user's password. This is one of the main problems with the standard password authentication mechanism that GridAdvanced solves. Users can freely authenticate with a system in a hostile environment and the chances of an attacker learning their password after that authentication is extremely small.

After an observation the expected number of possible Grid Passwords from which an attacker can choose his or her guess is reduced. To calculate the expected number of passwords an attacker can guess from, we must consider the correct corner and the other three corners separately. The expected number of passwords that an attacker can guess from considering only the correct corner is:

$$\left(1 + \frac{P-1}{\pi}\right)^N$$

This is because we know that the correct GridPass appears in the set of possible Grid Passwords for this corner. Therefore, to account for the correct GridPass character being in the set, we add a 1 in the first part of the numerator in Equation (4). Because the correct GridPass character has been accounted for, there remains 1 fewer GridCells to consider, hence the  $P - 1$ . The expected number of GridPass characters for each position is multiplied together for all  $N$  of the GridPass characters resulting in Equation (4).

For the remaining corners we are not assured that the observed GridCode digit will appear in any of the corners. Instead we calculate the expected number of Grid Passwords given a random GridCode. This expected value is almost the same as in Equation (4), however the special case is not considered.

$$\left(\frac{P}{\pi}\right)^N \times 3$$

To obtain the total expected number of possible passwords that an attacker can guess from, we need only sum Equation (4) and (5). This results in the following expected value:

$$\left(1 + \frac{P-1}{\pi}\right)^N + \left(\frac{P}{\pi}\right)^N \times 3 = 89,697,536$$

Therefore, if an attacker is given  $k = 3$  attempts to guess the correct password after observing a correct authentication, the attacker will have a 100% probability of knowing the correct password on a standard password authentication system. With the GridAdvanced this probability drops significantly.

$$\frac{3}{89,697,536} = \frac{1}{29,899,179}$$

## 4 Probability of Success With DecoyDigits

While the previous section demonstrated how secure GridAdvanced is without DecoyDigits, this section discusses how secure GridAdvanced is with the use of DecoyDigits. In most situations it is usually more beneficial to allow users to include DecoyDigits in their GridCode. This makes it much harder for someone who observes a valid authentication to discover the Grid Password. The probabilities discussed in the following sections build upon those derived in Section 3. It should be noted that only GridAdvanced is discussed in this section as there is no analog to DecoyDigits in the standard password scheme.

## 4.1 Random Guess of the Password

Because DecoyDigits do not have any affect on the GridPass, the probability of an attacker successfully guessing the GridPass after  $k$  attempts is the same as in Equation (2). Therefore, the addition of DecoyDigits does not change the probability of a successful attack for this scenario.

## 4.2 Random Guess of a Proper Authentication

As stated in the attack scenario, it is assumed that the attacker knows the inner workings of the system. Therefore, we can assume that the attacker knows the ratio of DecoyDigits to GridCode Digits. For the purposes of this paper we will assume that the ratio is the standard one DecoyDigit to every three GridCode Digits.

By allowing DecoyDigits the attacker is able to leverage the fact that “free” GridCode characters can be inserted without penalty if they are wrong. Therefore, the expected number of possible GridCodes is reduced to the following where  $A = [N * D] + N = 10$  for the purposes of this paper.

$$\left[ P^N / \binom{A}{N} \right]$$

Equation (8) expresses the expected number of possible passwords because in a single guess  $\binom{A}{N}$  GridCodes can be tested<sup>2</sup>. While this number is not exact because you can't always test  $\binom{A}{N}$  GridCodes in each attempt, it is larger than the actual number of possible GridCodes. Therefore, it is a safe approximation to use.

The probability of an attacker successfully guessing a valid GridCode, given a DecoyDigit ratio of 1:3, is given by:

$$\frac{k}{\left[ P^N / \binom{A}{N} \right]} = \frac{1}{\left[ 10^8 / \binom{10}{8} \right]} = \frac{1}{2,222,222}$$

## 4.3 Observing an Authentication

The equation used to determine the number of possible passwords without DecoyDigits can be modified slightly to determine the number of possible passwords with DecoyDigits. The exponent in Equation (7) need only be changed from  $N$  to  $A$  to determine the number of possible passwords including DecoyDigits. Therefore, the number of possible passwords after observing a valid authentication is

$$\frac{3}{\left( 1 + \frac{P-1}{P} \right)^A + \left( \frac{P}{P} \right)^A \times 3} = \frac{1}{2,113,132,488}$$

## 5 Conclusion

GridAdvanced provides the security of a one-time password with the ease-of-use of a standard password authentication mechanism. GridAdvanced is extremely beneficial in places where a user must authenticate with a system and the user does not have control over the environment.

Table 1 provides a comparison between the standard password authentication scheme and GridAdvanced for each of the attack scenarios described in Section 2. One should note that while it appears as though the standard password authentication scheme is stronger

<sup>2</sup>  $\binom{a}{b}$  is the standard choose notation representing  $\frac{a!}{b!(a-b)!}$



than GridAdvanced when only an authentication is required, in the case of the GridAdvanced the attacker is only able to authenticate once. However, the most important point to note is that GridAdvanced provides a much, much stronger level of security when a valid authentication has been observed by the attacker.

Table 1: A summary of the probabilities for the different attack scenarios between a standard password authentication scheme and the GridAdvanced authentication scheme with and without DecoyDigits. Assumes 80 possible characters in the password (upper and lower case letters, numbers, symbols), a password length of 8 characters, and two additional DecoyDigits where applicable.

Attack Scenario	GridAdvanced	GridAdvanced	Static Password
	w/o Decoys	with Decoys	
Guess of the Password	$\frac{1}{2,236,962,133,333,333}$	$\frac{1}{2,236,962,133,333,333}$	$\frac{1}{559,240,533,333,333}$
Guess of a GridCode	$\frac{1}{100,000,000}$	$\frac{1}{2,222,222}$	$\frac{1}{1,677,721,600,000,000}$
Guess of the password after observing an authentication	$\frac{1}{29,899,179}$	$\frac{1}{2,113,132,488}$	$\frac{1}{1}$



## 6 Appendix A: Example GridAdvanced Interfaces

Figure 3: QWERTY-style grid with 80 cells

Enter GridCode™:  
[GridCode™ - How To?](#)  
gridguard Login  
Manage GridPass™  
Logout  

1 2 3  
4 5 6  
7 8 9  
0 CE

Choose MyGrid™  
-default-  
Select  
U.S. Patented No. 7,143,440

4	5	7	0	1	0	4	9	9	9	4	8	4	2	3	4	7	8	9	8
!	@	#	\$	%	^	&	*	(	)										
0	5	2	5	4	7	2	4	2	7	5	7	4	6	8	8	6	4	4	2
1	1	5	6	2	3	1	7	8	1	7	0	4	2	0	1	6	1	7	6
9	4	3	7	8	4	3	6	9	4	5	6	5	4	4	0	1	2	0	2
2	5	8	0	2	3	4	0	2	0	7	1	1	0	6	1	9	7	9	8
Q	W	E	R	T	Y	U	I	O	P										
6	8	3	3	5	4	9	1	6	2	5	1	7	1	1	6	3	1	2	1
8	0	3	8	4	2	9	7	1	5	0	0	3	9	2	3	5	7	3	1
A	S	D	F	G	H	J	K	L	:										
9	5	9	2	4	9	8	0	9	6	5	9	6	0	5	9	3	8	7	1
0	2	2	4	7	0	9	9	3	9	6	1	1	5	5	2	5	1	6	8
9	7	7	8	0	1	9	2	1	6	1	4	1	2	6	8	2	5	0	0
6	0	8	8	5	5	9	3	7	4	4	7	3	4	1	7	7	4	6	2
q	w	e	r	t	y	u	i	o	p										
2	4	0	3	7	0	9	6	4	1	3	9	5	8	6	2	0	1	7	9
5	3	5	5	9	4	1	6	8	9	5	5	8	1	8	5	2	4	5	0
a	s	d	f	g	h	j	k	l	;										
9	1	7	7	3	4	8	3	0	5	4	2	2	0	4	4	4	4	9	
5	4	4	9	3	5	7	9	7	1	7	8	8	6	9	7	5	9		
z	x	c	v	b	n	m	,	.	/										
2	9	2	9	8	2	9	6	6	8	6	7	9	3	5	0	6	2	7	7

Figure 4: 99-cell Grid with additional symbols and special characters

Enter GridCode™:  
[GridCode™ - How To?](#)  
gridguard Login  
Manage GridPass™  
Logout  

1 2 3  
4 5 6  
7 8 9  
0 CE

Choose MyGrid™  
-default-  
Select  
U.S. Patented No. 7,143,440

0	5	7	0	7	4	7	9	3	8	4	0	7	1	2	7	7	3	0	0	9	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	1	2	3			
8	1	3	5	8	2	2	1	6	9	5	2	6	5	8	9	7	9	4	1	3	
8	1	4	0	0	4	0	8	4	7	8	0	4	0	1	6	3	8	9	0	6	8
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	4	5	6			
4	2	6	1	6	6	7	0	8	9	0	8	2	8	4	9	0	4	0	2	5	3
1	6	8	0	0	9	0	7	6	5	9	6	2	3	4	0	9	2	2	3	1	5
Q	R	S	T	U	V	W	X	Y	Z	<	>	/	?	;	:	7	8	9			
4	4	6	6	9	0	8	9	8	5	8	3	3	6	3	5	6	4	7	3	2	8
8	5	0	9	0	2	8	5	6	2	2	9	4	9	1	4	4	3	8	7	3	4
7	1	0	0	2	2	2	2	9	4	0	2	1	0	7	5	1	1	2	1	8	0
5	3	0	5	1	0	7	6	1	3	3	4	6	3	3	0	1	5	6	3	4	7
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	!	@	\$			
7	6	2	4	6	5	8	9	6	7	6	8	1	1	6	2	6	2	4	7	3	0
6	7	6	5	9	5	2	4	7	2	8	2	5	9	4	0	2	9	6	9	6	8
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	%	^	&			
9	5	2	9	7	1	7	2	0	9	4	1	4	7	0	2	3	0	1	7	8	5
2	7	2	4	4	2	5	1	7	3	6	7	1	7	8	2	0	3	7	4	8	6
q	r	s	t	u	v	w	x	y	z	[	]	{	}	<	>	-	_	=			
0	8	2	8	4	6	8	2	4	3	1	4	5	9	5	6	5	0	8	8	8	2
4	3	2	2	8	3	0	5	9	5	2	6	0	2	8	5	5	9	6	0	7	1
7	5	9	1	1	1	4	8	9	6	5	4	2	2	2	2	6	8	6	3	7	6
3	6	9	1	9	5	5	5	6	8	5	9	4	5	7	7	0	9	7	7	3	2
\		~	,	.	£	space	¥	€								0	7	0	1	5	2
8	8	3	7	4	2	5	9	0	4	0	8	6	6	9	2	0	7	0	1	5	2