WHAT IS CLAIMED IS:

1. A security authentication method comprising:

establishing a user account associated with a login credential;

generating an encryption salt;

generating graphical key images of a plurality of sequences of values each beginning at a random point;

generating encrypted key values by encrypting each value in the plurality of sequences using the generated encryption salt;

incorporating the graphical key images and encrypted key values into a displayable input form;

receiving user input from a user including a plurality of encrypted key values;

generating decrypted key values by decrypting the encrypted key values of the user input using the encryption salt; and

giving the user access to data associated with the user account in response to the decrypted key values matching the login credential.

2. The security authentication method of claim 1, further comprising displaying the input form including the graphical key images and encrypted key values to the user using an electronic device.

3. The security authentication method of claim 2, wherein displaying the input form further comprises displaying the plurality of graphical key images in a rotary dial graphical representation.

4. The security authentication method of claim 3, further comprising enabling the user to enter the login credential by clicking on the displayed graphical key images.

5. The security authentication method of claim 1, further comprising receiving a request for randomized security data at a security authentication server from a server hosting data associated with the user account.

6. The security authentication method of claim 5, further comprising:

transmitting the randomized security data including the graphical key images and encrypted key values to the server;

generating the displayable input form incorporating the graphical key images and encrypted key values at the server;

transmitting the displayable input form to an electronic device used by the user; and

displaying the input form at the electronic device.

7. The security authentication method of claim 6, wherein transmitting the randomized security data comprises transmitting a location reference of the graphical key images to the server.

8. A security authentication method comprising:

establishing a user account associated with a login credential;

generating an encryption salt;

generating graphical key images of a plurality of sequences of values each beginning at a random point;

generating encrypted key values by encrypting each value in the plurality of sequences using the generated encryption salt;

incorporating the graphical key images and encrypted key values into a displayable input form;

receiving user input including a plurality of encrypted key values;

generating decrypted key values by decrypting the encrypted key values of the user input using the encryption salt; and

verifying that the decrypted key values match the login credential.

9. A security authentication system comprising:

a security authentication server operable to:

establish a user account associated with a login credential;

generate an encryption salt;

generate graphical key images of a plurality of sequences of values each beginning at a random point;

generate encrypted key values by encrypting each value in the plurality of sequences using the generated encryption salt;

a server operable to:

receive the graphical key images and encrypted key values from the security authentication server; and

incorporate the graphical key images and encrypted key values into a displayable input form; and

an electronic device operable to:

display the input form;

receive user input from a user including a plurality of encrypted key values; and

the security authentication server further operable to:

receive the user input from the server;

generate decrypted key values by decrypting the encrypted key values of the user input using the encryption salt;

verifying the decrypted key values with the login credential; and

notifying the server of successful authentication.

10. The system of claim 9, wherein the electronic device is operable to display the input form in the form of rotary dials incorporating the graphical key images of the sequences of values.

11. The system of claim 10, wherein the electronic device is operable to enable the user to enter the login credential by clicking on the displayed graphical key images.

12. The system of claim 9, further comprising giving the user access to data associated with the user account in response to the decrypted key values matching the login credential.

13. A security authentication system comprising:

means for establishing a user account associated with a login credential;

means for generating an encryption salt;

means for generating graphical key images of a plurality of sequences of values each beginning at a random point;

means for generating encrypted key values by encrypting each value in the plurality of sequences using the generated encryption salt;

means for incorporating the graphical key images and encrypted key values into a displayable input form;

means for receiving user input including a plurality of encrypted key values;

means for generating decrypted key values by decrypting the encrypted key values of the user input using the encryption salt; and

means for verifying that the decrypted key values match the login credential.

14. A security authentication method comprising:

transmitting a request for login into a user account to a web server;

receiving an input form from the web server having graphical key images of a plurality of sequences of values and encrypted key values;

displaying the input form in a rotary dial format;

receiving user input entered using the input form; and

transmitting encrypted key values representing the user input to the web server for authentication.

WHAT IS CLAIMED IS:

1. A method for performing a security authentication, the method comprising:

receiving, by a computing device, a username of a user along with a request for randomized security data in conjunction with a request by the user to access a resource, and in response, generating, by the computing device, N sequences, each sequence including a same M unique digits, each sequence beginning with a different digit of the M digits, the digits in each sequence being sequenced in a same order as the digits in each other sequence subject to the first digit in each sequence being considered as sequentially after the last digit in each sequence, N being at least 2, M being at least 3;

generating, by the computing device, an encrypted value specific to each of the digits in the N sequences;

transmitting, by the computing device, the username, the N sequences, and the generated encrypted values to a destination device that permits the user to select a digit from each of the N sequences;

after the transmitting, receiving, by the computing device from the destination device, N encrypted values of the transmitted encrypted values, wherein an received encrypted value of the N received encrypted values is specific to one of the digits selected by the user, at an electronic device, from a respective I^{th} sequence of the N sequences (I=1, 2, . . . , N); and

determining, by the computing device, N digits respectively specific to the received N encrypted values and that the determined N digits form a number matching a PIN associated with the username, which authenticates the user to access the resource.

2. The method of claim 1, wherein in further response to the receiving the username along with the request for randomized security data, generating, by the computing device, a string of random bits of a predetermined length, and wherein the generating the encrypted value comprises generating the encrypted value in association with each unique digit in the N sequences using the string of random bits.

3. The method of claim 1 or 2, wherein the generating the encrypted value specific to each of the digits in the N sequence results in only M encrypted values being generated for the N sequences collectively.

4. The method of claim 1, 2 or 3, further comprising:

randomly selecting, by the computing device, a digit of the digits in each sequence to denote where each sequence begins, which results in each sequence beginning with the different digit.

5. The method of any one of the preceding claims, wherein the transmitting the username, the N sequences, and the generated encrypted values further comprises transmitting to the destination device a location reference denoting where the N sequences are stored.

6. The method of any one of the preceding claims, wherein the computing device, the destination device, and the electronic device are distinct devices connected to and separated from one another by a network.

7. The method of any one of the preceding claims, further comprising:

providing, by the destination device, the user with access to the resource in response to the determining that the N digits form the number matching the PIN.

8. The method of any one of the preceding claims, further comprising:

sending, by the destination device to the electronic device, a web page that includes an entry for the user to enter the username.

9. The method of any one of the preceding claims, further comprising:

incorporating, by the destination device, the N sequences and the generated encrypted values into an input form, wherein the input form is configured to be displayed to the user for receiving from the user an identification of the digits selected by the user from each of the N sequences.

10. The method of claim 9, wherein the input form is configured to have the N sequences displayed in a rotary dial graphical representation.

11. A computer program product for performing a security authentication, the computer program product comprising one or more computer-readable storage devices and program instructions stored on the one or more storage devices, wherein the program instructions comprise:

program instructions to receive, by a computing device, a username of the user along with a request for randomized security data in conjunction with a request by the user to access a resource, and in response, generate N sequences, each sequence including a same M unique digits, each sequence beginning with a different digit of the M digits, the digits in each sequence being sequenced in a same order as the digits in each other sequence subject to the first digit in each sequence being considered as sequentially after the last digit in each sequence, N being at least 2, M being at least 3;

program instructions to generate an encrypted value specific to each of the digits in the N sequences;

program instructions to transmit the username, the N sequences, and the generated encrypted values to a destination device that permits the user to select a digit from each of the N sequences;

program instructions to receive, by the computing device from the destination device after the N sequences and the encrypted values have been transmitted to a destination device, N encrypted values of the transmitted encrypted values, wherein an I^{th} received encrypted value of the N received encrypted values is specific to one of the digits selected by the user, at an electronic device, from a respective I^{th} sequence of the N sequences (I=1, 2, . . . , N); and

program instructions to determine, by the computing device, N digits respectively specific to the received N encrypted values and that the N digits form a number matching a PIN associated with the username, which authenticates the user to access the resource.

12. The computer program product of claim 11, wherein the program instructions further comprise:

program instructions to, in further response to the receiving the username along with the request for randomized security data, generate, by the computing device, a string of random bits of a predetermined length, wherein the program instructions to generate the encrypted value comprises program instructions to generate the encrypted value in association with each unique digit in the N sequences using the string of random bits.

13. The computer program product of claim 11 or 12, wherein the program instructions to generate the encrypted value specific to each of the digits in the N sequence results in only M encrypted values being generated for the N sequences collectively.

14. The computer program product of claim 11, 12 or 13, wherein the program instructions further comprise:

program instructions to randomly select, by the computing device, a digit of the digits in each sequence to denote where each sequence begins, which results in each sequence beginning with the different digit.

15. The computer program product of any one of claims 11 to 14, wherein the program instructions to transmit the username, the N sequences, and the generated encrypted values further comprises program instructions to transmit to the destination device a location reference denoting where the N sequences are stored.

16. A computer system for performing a security authentication, the system comprising one or more processors, one or more computer-readable memories, one or more computer-readable storage devices, and program instructions stored on the one or more storage devices for execution by the one or more processors via the one or more memories, wherein the program instructions comprise:

program instructions to receive, by a computing device, a username of a user along with a request for randomized security data in conjunction with a request by the user to access a resource, and in response, generate N sequences, each sequence including a same M unique digits, each sequence beginning with a different digit of the M digits, the digits in each sequence being sequenced in a same order as the digits in each other sequence subject to the first digit in

each sequence being considered as sequentially after the last digit in each sequence, N being at least 2, M being at least 3;

program instructions to generate an encrypted value specific to each of the digits in the N sequences;

program instructions to transmit the username, the N sequences, and the generated encrypted values to a destination device that permits the user to select a digit from each of the N sequences;

program instructions to receive, by the computing device from the destination device after the N sequences and the encrypted values have been transmitted to a destination device, N encrypted values of the transmitted encrypted values, wherein an I^{th} received encrypted value of the N received encrypted values is specific to one of the digits selected by the user, at an electronic device, from a respective I^{th} sequence of the N sequences (I=1, 2, . . . , N); and

program instructions to determine, by the computing device, N digits respectively specific to the received N encrypted values and that the N digits form a number matching a PIN associated with the username, which authenticates the user to access the resource.

17. The computer system of claim 16, wherein the program instructions further comprise:

program instructions to, in further response to the receiving the username along with the request for randomized security data, generate, by the computing device, a string of random bits of a predetermined length, wherein the program instructions to generate the encrypted value comprises program instructions to generate the encrypted value in association with each unique digit in the N sequences using the string of random bits.

18. The computer system of claim 16 or 17, wherein the program instructions to generate the encrypted value specific to each of the digits in the N sequence results in only M encrypted values being generated for the N sequences collectively.

19. The computer system of claim 16, 17 or 18, wherein the program instructions further comprise:

program instructions to randomly select, by the computing device, a digit of the digits in each sequence to denote where each sequence begins, which results in each sequence beginning with the different digit.

20. The computer system of any one of claims 16 to 19, wherein the program instructions to transmit the username, the N sequences, and the generated encrypted values further comprises program instructions to transmit to the destination device a location reference denoting where the N sequences are stored.