CLAIMS

1. A decryption method comprising:

receiving a user input which includes a password component and a non-password component that is defined by a user or a user device, wherein the non-password component includes a plurality of characters ~~is~~which are arranged relative to the password component in a random manner and at least some of the plurality of characters are arranged relative to the password component in a predefined sequence to reflect a predetermined information determined by the user;

verifying a presence of a pre-assigned password within the user input, wherein the pre-assigned password is associated with the user and stored in a first database; and

based on the verified presence of the pre-assigned password within the user input, identifying the non-password component.

2. The method of claim 1, further comprising:

ascertaining a validity of the user input by comparing the non-password component against a second database which includes a plurality of historical non-password components of the user; and

establishing the user input is valid and storing the non-password component in the second database if the non-password component does not correspond to any of the plurality of historical non-password components.

3. The method of claim 1, wherein the pre-assigned password includes a plurality of characters provided in a non-defined sequence, and wherein verifying a presence of a pre-assigned password includes verifying a presence of all the plurality of characters of the pre-assigned password in the user input.

4. The method of claim 1, wherein the pre-assigned password includes

a plurality of sub-passwords, each sub-password including a plurality of characters provided in a predefined sequence,

wherein verifying a presence of a pre-assigned password includes verifying a presence of all of the plurality of characters of each sub-password within the user

input and verifying an aggregation of the verified characters corresponding to each sub-password conforms to the corresponding predefined sequence of the each sub-password.

5. A non-transitory computer readable medium encoded with program code operable, when loaded on a computer, to effect the method of any of claims 1 to 4.

6. An encryption method comprising:

generating, by a computing device, a password component from a plurality of characters of a pre-assigned password which is associated with a user; and

randomly inserting, by the computing device, a non-password component into the generated password component;

wherein the non-password component includes ~~at least one~~a plurality of variable characters, and at least some of the plurality of variable characters are arranged relative to the password component in a predefined sequence to reflect certain predetermined information~~.~~

7. The method of claim 6, wherein the pre-assigned password includes a plurality of sub-passwords, each sub-password having a plurality of characters provided in a predefined sequence,

wherein generating a password component includes:

dividing, by the computing device, each sub-password into a plurality of subsets,

wherein randomly inserting a non-password component includes:

interposing, by the computing device, the subsets of one sub-password with the subsets of at least another sub-password, wherein an aggregation of the interposed subsets of each sub-password conforms to the corresponding defined sequence of the each sub-password.

8. The method of claim 6, wherein the pre-assigned password includes a plurality of characters in a non-defined sequence, and

wherein generating a password component includes generating, by the computing device, a random permutation of the plurality of characters.

9. The method of any one of claims 6 to 8, wherein the certain predetermined information~~the non-password component includes at least one variable character to reflect~~ includes an evaluation of a service rendered between the check-in time and the check-out time and/or a monetary value determined by the user.

10. The method of any one of claims 6 to 8, ~~wherein the non-password component includes a plurality of variable characters,~~ wherein randomly inserting a non-password component includes:

inserting, by the computing device, the plurality of variable characters at non-adjacent positions in the generated password component.

~~11. The method of claim 10, wherein at least some of the variable characters are arranged in a sequence to reflect a pre-determined information determined by the user.~~

~~12~~11. The method of any one of claims 6 to 8, wherein the pre-assigned password or at least part of the pre-assigned password which is associated with the user is generated by a key token assigned to the user, or sent to the user by Short Message Service.

~~13~~12. A non-transitory computer readable medium encoded with program code operable, when loaded on a computer, to effect the method of any of claims 6 to ~~12~~11.

~~14~~13. A decryption system, comprising:

a computing device comprising a memory and a processor device communicatively coupled to the memory, and configured to execute program code stored in the memory, the program code comprising:

a verification module configured to:

verify a presence of a pre-assigned password within a user input which includes a password component and a non-password component that is

defined by a user or a user device, wherein the non-password component includes a plurality of characters ~~is~~ which are arranged relative to the password component in a random manner and at least some of the plurality of characters are arranged relative to the password component in a predefined sequence to reflect a predetermined information determined by the user, wherein the pre-assigned password is stored in a first database and associated with the user or the user device, and

identify the non-password component based on the verified presence of the pre-assigned password within the user input.

~~15~~14. The decryption system of claim ~~14~~13,

wherein the verification module is further configured to:

ascertain a validity of the user input by comparing the non-password component against a second database in which a plurality of historical non-password components of the user are stored,

establish the user input is valid if the non-password component does not correspond to any of the historical non-password components of the user, and

store the non-password component in the second database.

~~16~~15. The decryption system of claim ~~15~~14, wherein the first database and the second database are stored in the memory of the computing device.

~~17~~16. The decryption system of claim ~~14~~13, wherein the pre-assigned password includes a plurality of characters provided in a non-defined sequence, and

wherein the verification module is further configured to:

verify a presence of all the plurality of characters of the pre-assigned password in the user input.

~~18~~17. The decryption system of claim ~~14~~13, wherein the pre-assigned password includes a plurality of sub-passwords, each sub-password including a plurality of characters provided in a predefined sequence,

wherein the verification module is further configured to:

verify a presence of all of the plurality of characters of each sub-password within the user input, and

verify an aggregation of the verified characters corresponding to each sub-password conforms to the corresponding predefined sequence of the each sub-password.

~~19~~18. The decryption system of claim ~~14~~13,

wherein the verification module is further configured to:

ascertain a validity of the user input by comparing the input user against a third database in which a plurality of historical user inputs of the user are stored,

establish the user input is valid if the user input does not correspond to any of the plurality of historical user inputs, and

store the user input in the third database.

~~20~~19. An encryption system comprising:

a computing device comprising a memory and a processor device communicatively coupled to the memory, and configured to execute program code stored in the memory, the program code comprising:

an encryption module configured to:

generate a password component from a plurality of characters of a pre-assigned password, and

randomly insert a non-password component into the generated password component,

wherein the non-password component includes ~~at least one variable character~~ a plurality of variable characters, and at least some of the plurality of variable characters are arranged relative to the password component in a predefined sequence to reflect certain predetermined information.

~~21~~20. The encryption system of claim ~~20~~19, wherein the pre-assigned password includes a plurality of sub-passwords, each sub-password having a plurality of characters provided in a predefined sequence,

wherein the encryption module is further configured to:

divide each sub-password into a plurality of subsets, and

interpose the subsets of one sub-password with the subsets of at least another sub-password, wherein an aggregation of the interposed subsets of each sub-password conforms to the corresponding defined sequence of the each sub-password.

~~22~~21. The encryption system of claim ~~20~~19, wherein the pre-assigned password includes a plurality of characters in a non-defined sequence, and

wherein the encryption module is further configured to:

generate a random permutation of the plurality of characters.

~~23~~22. The encryption system of any one of claims ~~20~~ 19 to ~~22~~21, ~~wherein the non-password component includes a plurality of variable characters,~~

wherein the encryption module is further configured to:

insert the plurality of variable characters at non-adjacent positions in the generated password component.

~~24. The encryption system of claim 23, wherein the encryption module is further configured to:~~

~~arrange at least some of the variable characters in a sequence to reflect a pre-determined information determined by the user.~~