Dataflow

This document shows the dataflow in our project

signup

Form the username and password

Hashing of password and then storing it to DB

password -> hash then store to DB hashing key --> will be private to the server

```
sample key =
| X A P U F |
| N C G Y K |
| I Z E O M |
| B L W V R |
| D H Q T S |
```

hash function --> Gallant-56

NOTE*

> Gallant Hash is not an existing hash, it is a catchy name that we are giving to our hash function output of hash function will be of 56 letters

lenght of password = x letters

Delimiter password[x+1] = '$'

concatString (n-letters) n=56-(x+1)

concatString: i = [0, n-1]

```
concatString[i] = addStr [ (floor((((i*4)^2)/3)))%16 ];
password.concat(concat-string);
```

> apply bifid cipher now to find the encrypted hash

```
addStr = {
        0: m,
        1: f,
        2: g,
        3: e,
        4: r,
        5: y,
        6: z,
        7: q,
        8: r,
        9: g,
        10: i,
        11: o,
        12: a,
        13: q,
        14: e,
        15: s
};
```

EXAMPLE

```
password: "Madhav" + 50 random letters
password[7] = '$'
required letters = [8 to 55]
n = 56 - (6+1) = 49 letters
concatString = [0 to 48]

concatString[0] = addStr[(floor((((0*4)^2)/3)))%16] = addStr[0] = m
concatString[1] = addStr[(floor((((1*4)^2)/3)))%16] = addStr[5] = y
....
....
....
password.concat(concatString)
```

Now the password will be of 56 letters

> Now apply bifid to find the encrypted hash of the given password
>
> > Store the password to the DB