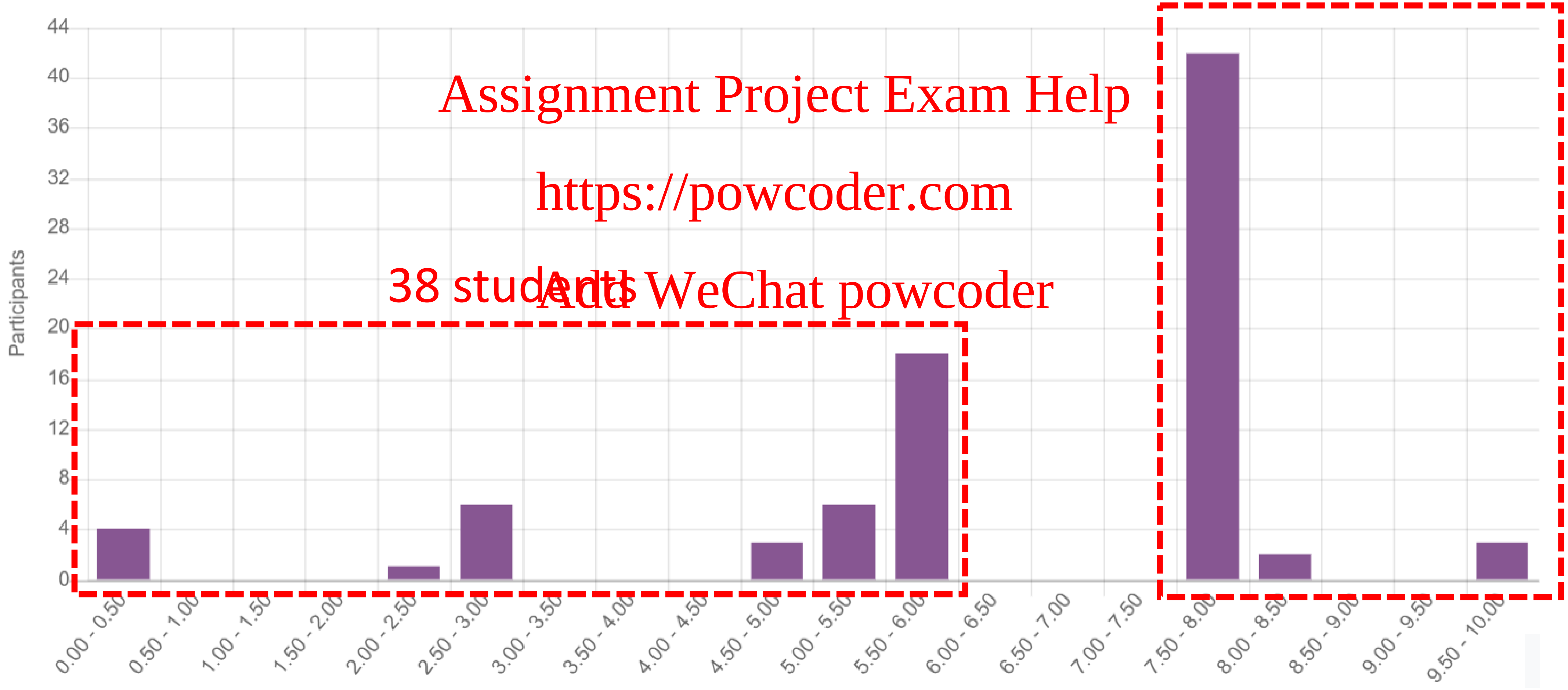
Quiz 7 - statistics

# of participants: 85 / 100

average: 7.344 / 10

47 students got A+



38 students

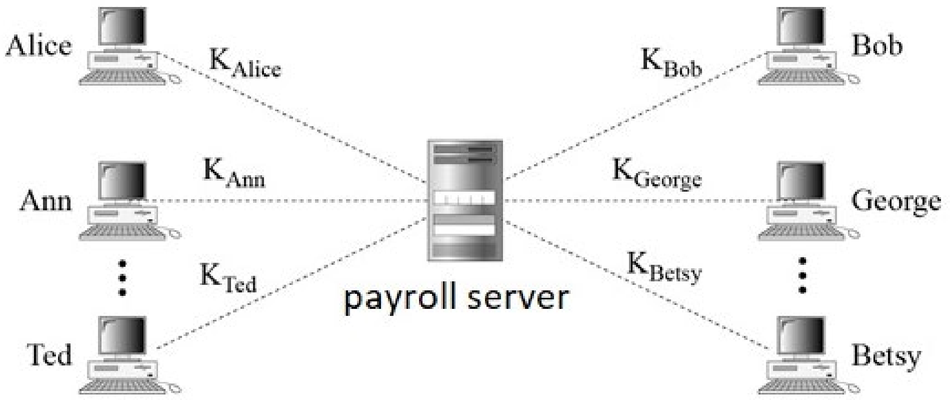
7.5*1.2 = 9.0

Assume we are designing a payroll server in a system of N users/employees.
We would like the server to be able to send confidential updates to each of the N employees about their monthly earnings. No other messages in this system need to be protected (i.e., encrypted). The actual distribution of keys (either symmetric or asymmetric) is also not an issue in this system.

Which of the following do you agree with, when it comes to the design of the given payroll server?

1) The server should deploy asymmetric encryption, as that would reduce the overall number of keys that the server needs to have and use compared to symmetric encryption.

2) The asymmetric encryption does not provide any advantage in terms of the number of keys used by the server, yet it is slower. So, symmetric encryption is the way to go.



Symmetric encryption:
To send confidential message to all N users, the server has to have a unique symmetric key for each user. N keys in total!

Asymmetric encryption:
To send confidential message to all N users, the server has to have the public key of/for each of the N users. N keys in total!

Consider an asymmetric encryption system with N users, including Alice and Bob.
Alice and Bob have provided everybody else with their respective public keys ($K_{A\text{-public}}$ and $K_{B\text{-public}}$), while keeping their private keys for themselves ($K_{A\text{-private}}$ and $K_{B\text{-private}}$).

Now, Alice wants to send a confidential message M to Bob, while at the same time enabling Bob to verify that the message was sent by her/Alice (and not someone else pretending to be Alice).

How should Alice encrypt such a message?

Alice does not have this key!

1) First encrypt M with $K_{B\text{-private}}$ and then with $K_{A\text{-private}}$ - i.e., Alice sends $K_{A\text{-private}}(K_{B\text{-private}}(M))$

2) First encrypt M with $K_{B\text{-private}}$ and then with $K_{A\text{-public}}$ - i.e., Alice sends $K_{A\text{-public}}(K_{B\text{-private}}(M))$

Bob cannot decrypt this!

3) First encrypt M with $K_{B\text{-public}}$ and then with $K_{A\text{-public}}$ - i.e., Alice sends $K_{A\text{-public}}(K_{B\text{-public}}(M))$

4) First encrypt M with $K_{B\text{-public}}$ and then with $K_{A\text{-private}}$ - i.e., Alice sends $K_{A\text{-private}}(K_{B\text{-public}}(M))$

Alice and Bob are trying to establish a new symmetric encryption key using the Diffie-Hellman algorithm/procedure as discussed in class. They adopt the following values for p and g: **p=9 and g=2**.

Alice’s chooses her private key to be **$K_{A\text{-private}}$ = 2,** and Bob chooses his private key to be **$K_{B\text{-private}}$ = 3.** What will their new symmetric key be, once they go through the entire Diffie-Hellman procedure?

[✓ 1) 1]

2) 2

3) 4

4) 8

$$K_{A\text{-public}} = 2^2 \text{ mod } 9 = 4$$

$$K = (K_{A\text{-public}})^{K_{B\text{-private}}} \text{ mod } 9$$

Alice and Bob are trying to establish a new symmetric encryption key using the Diffie-Hellman algorithm/procedure as discussed in class. They adopt the following values for p and g: **p=9 and g=2**.

Trudy knows the values of p and g, and she also manages to capture Alice's public key: **$K_{A\text{-public}}$ = 4**.

Given these assumptions, which of the following is correct?

1) Trudy concludes that Alice's private key must be $K_{A\text{-private}} = 2$.

66.6% of the grade

2) Trudy concludes that Alice's private key must be $K_{A\text{-private}} = 4$.

3) Trudy concludes that Alice's private key must be $K_{A\text{-private}} = 6$.

4) One of the above statements is partially correct.

$K_{A\text{-public}} = 2^k \bmod 9$

2^k mod 9	1	2	4	8	7	5	1	2	4
2^k	1	2	4	8	16	32	64	128	256
k	0	1	2	3	4	5	6	7	8