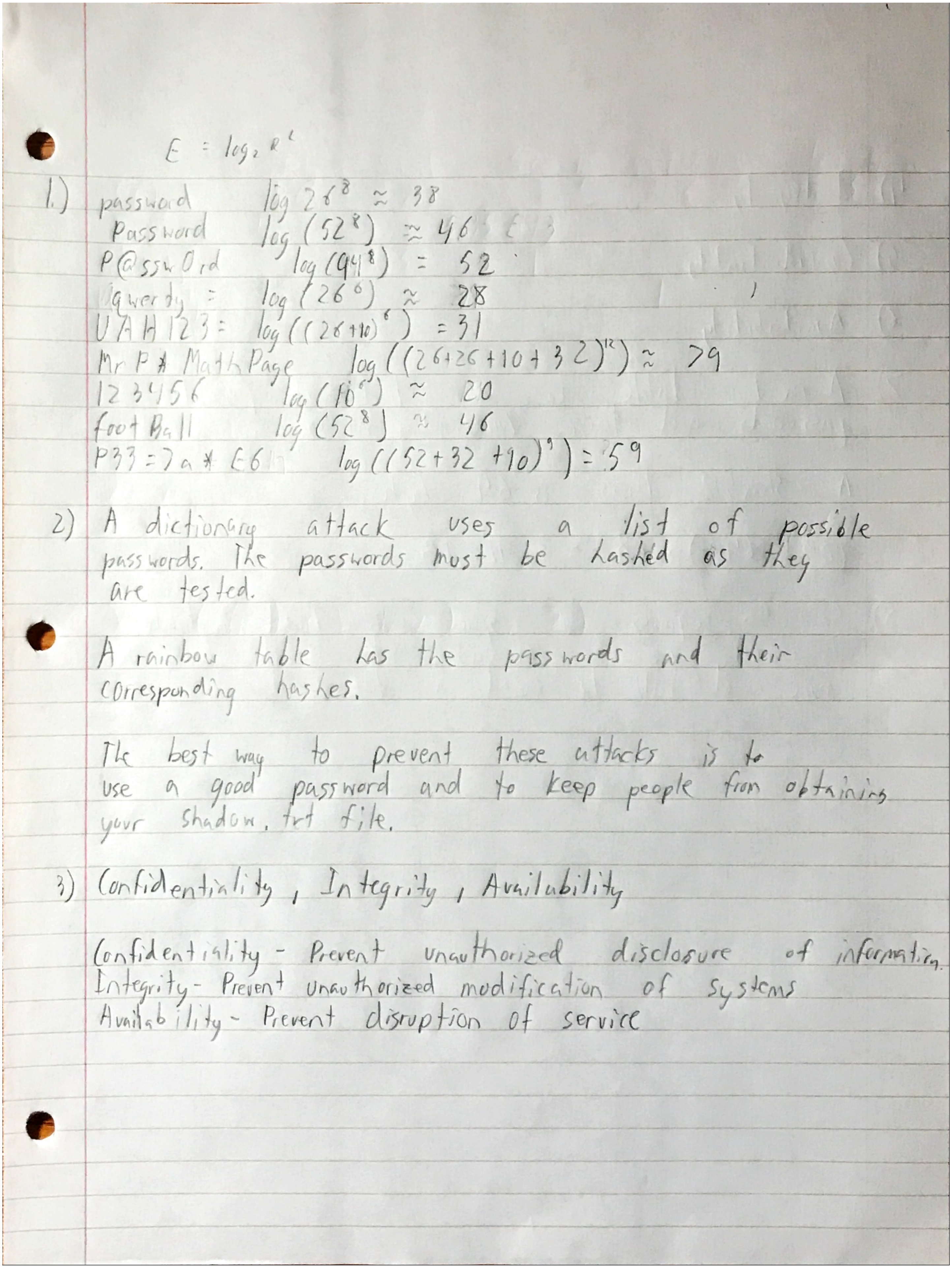


$E = \log_2 R^L$

1.)

password	$\log 26^8 \approx 38$
Password	$\log(52^8) \approx 46$
P@ssw0rd	$\log(94^8) = 52$
qwerty =	$\log(26^6) \approx 28$
UAH123 =	$\log((26+10)^6) = 31$
MrP*MathPage	$\log((26+26+10+32)^{12}) \approx 79$
123456	$\log(10^6) \approx 20$
footBall	$\log(52^8) \approx 46$
P33=7a*E6	$\log((52+32+10)^9) = 59$

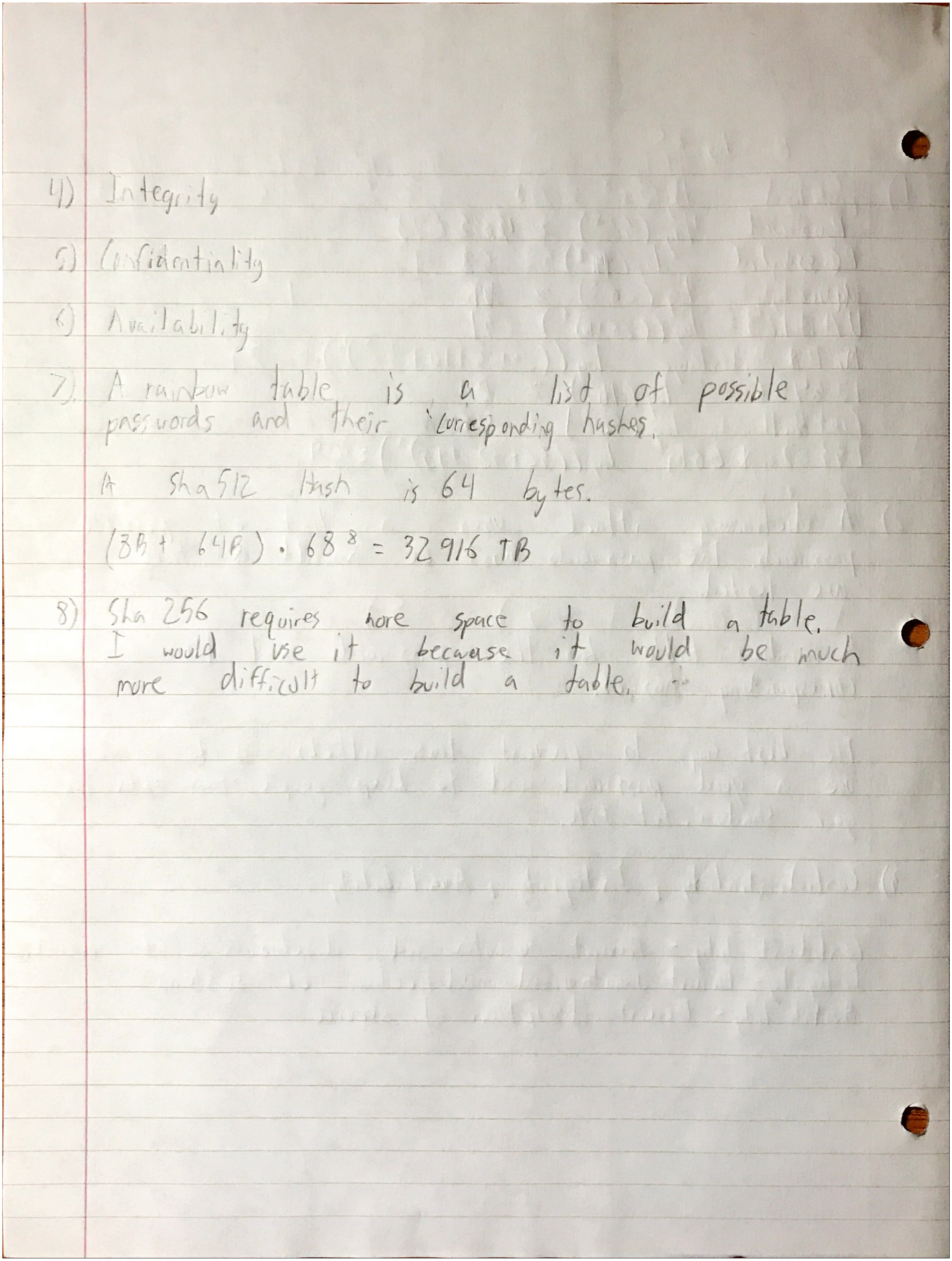
2) A dictionary attack uses a list of possible passwords. The passwords must be hashed as they are tested.

A rainbow table has the passwords and their corresponding hashes.

The best way to prevent these attacks is to use a good password and to keep people from obtaining your shadow.txt file.

3) Confidentiality, Integrity, Availability

Confidentiality - Prevent unauthorized disclosure of information.
Integrity - Prevent unauthorized modification of systems
Availability - Prevent disruption of service



4) Integrity

5) Confidentiality

6) Availability

7) A rainbow table is a list of possible passwords and their corresponding hashes.

A Sha512 Hash is 64 bytes.

$(8B + 64B) \cdot 68^8 = 32916\ TB$

8) Sha 256 requires more space to build a table. I would use it because it would be much more difficult to build a table.