5 Bias, privacy, and safe computing – Part 2

Name: _____ Class: _____ Date: _____

Recall

In Part A you met the effects of computing. Now fairness and keeping data safe:

- Programs can be unfair if they learn from unfair data.
- Your personal information needs protecting.
- Messages can be scrambled so only the right person can read them.

Each idea has a worked example before the Practice.

New ideas

1 Computing bias

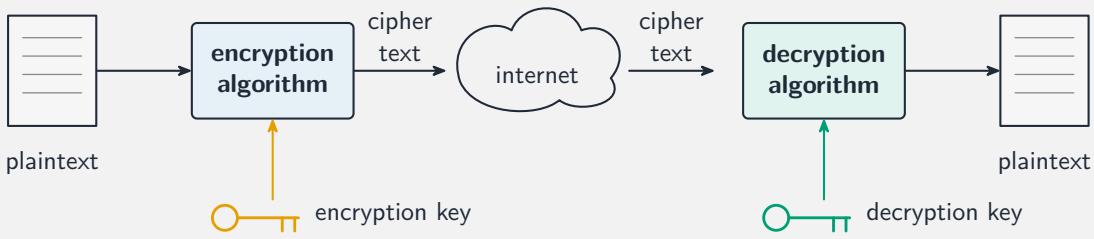
A program can carry **bias** if the data it learns from does not represent everyone fairly –leading to unfair results for some groups. The bias comes from the data and design, not the machine ”deciding” to be unfair.

2 Privacy

Programs that collect data raise **privacy** concerns. Good practice: collect only what is needed, protect it, and be honest about how it is used.

3 Encryption

Encryption scrambles data so that only someone with the right key can read it – keeping messages and passwords safe as they travel over the internet.



4 Safe computing

Protect yourself with strong, unique passwords, caution with unknown links and downloads, and keeping software up to date.

> **Watch out:** computing bias usually comes from **biased data**, not a machine choosing to be unfair. If a program is trained on data that under-represents some people, it can treat them unfairly –so the fix is better data and design.

Practice

Try these in order. The methods are all above.

2.1 State where computing bias usually comes from. [2]

2.2 State two good practices for handling people's personal data. [2]

2.3 State what encryption does. [2]

2.4 Give two ways to stay safe online. [2]

2.5 Explain why a program trained on unfair data can give unfair results. [2]