December 5, 2015

Dear Participant,
Welcome to the secret messages challenge! Computer scientists use secret codes and other tricks of *cryptography* to keep your information secure and private online, even if people are watching the messages you send. People have been using cryptography for centuries to hide their messages from spies, enemies, or even curious family members! This packet has some examples of cryptographic techniques from the past.

The message on page 2 (which contains important information for page 5) is encrypted with a Caesar cipher: a type of secret code where every letter of the alphabet is shifted by a certain number. For example, a Caesar cipher of shift 3 turns ABC into DEF and a Caesar cipher of shift 13 turns ABC into MNO. It's supposedly named for Julius Caesar because the Romans used this in battle! Secret codes offer *confidentiality*: they keep your message secret from anyone except the recipient - unless of course someone breaks your code!

Page 3 and 4 each have two messages, one fake and one real on each page. Can you figure out which is which? People use a variety of techniques to ensure the *authenticity* (came from the right person) and *integrity* (nobody modified the message in transit) of their messages. Can you think of some other strategies besides the ones used here? If an attacker knew your strategy, what could they do to get around it and trick the recipient?

The message on page 5 is hidden in a story that doesn't sound very secret - can you find it? This technique of hidden messages is called steganography, and it was very common during World War II. People can hide messages inside text, pictures, music, and many other things. Sometimes steganography is combined with a secret code to hide the message further.

When you have solved the packet, bring your answers to us for a special prize!

Sincerely,

Security + Privacy Lab

Your friends in CSE's Security & Privacy Research Lab (https://seclab.cs.washington.edu)

Activity designed by: Anna Kornfeld Simpson, Ada Lerner, Lucy Simko, Eric Zeng, Camille Cobb, and Alex Takakuwa, all PhD students in the lab.

Ijhjrgjw 5, 2015

Ijfw Ufwynhnufsy,

Sty jajwd btwi ns ymj uzeeqj ts uflj knaj mfx ufwy tk ymj mniijs rjxxflj.

Xnshjwjqd,

Security + Privacy Lab

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

Write your answer here:

Only one of these messages is authentic, the other was not written by us.
Which message is real?
NOTE: Solve this before page 4!

December 5, 2015

Dear Participant,

The correct message on page four has an even number of words in it.

Sincereley,

Security & Privacy Lab

December 5, 2015

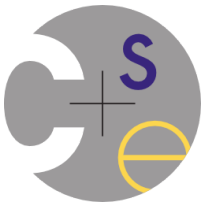
Dear Participant,

The correct message on page four has an odd number of words in it.

Sincerely,

Security + Privacy Lab

One of these messages was modified to say the wrong thing. Which message is correct?
NOTE: Solve page 3 first, it has an important clue!



Dear Participant,

Check out first letters of words on page five.

Good luck,
Security And Privacy Lab

Dear Participant,

Check out the last letters of words on page five.

Good luck,
Security And Privacy Lab

This story is how one cool engineer made computers flexible. To write instructions beyond arithmetic rote computations digitally, she made up the first compiler. But she is usually known for giving us the words bug and also debugging after scraping remains of a little bug mashed in an operating computer. And that was Grace Hopper.

Answer:

_ h e _ _ _ _ _ _ _ g _ _ _ _ _ _ o _ _.