Mathematical Insights in Computing

Intro to Cryptography: The One-Time Pad

1.) Your friend Alyssa P. Hacker has sent you a secret message, encrypted with a one-time pad! One week ago, she slipped you this piece of paper in the hallway:

One-Time Pad –

THISWASATRIUMPHYAY

Today, she slipped you another piece of paper:

Encrypted Message –

ZJMMEMQSOXKYWQKCGG

Alyssa subtracted the one-time pad from the decrypted message in order to get the encrypted message, and wrapped around at 26 letters. (It's like a Caesar cipher, but each letter gets a different shift.) A is 0, B is 1, C is 2, and so on, up until Z which is 25.

So, for example, the first letter of Alyssa's message is S. Adding T (19) to Z (25) results in S (18) mod 26.

What is the rest of the message?

Decrypted Message –

S

2.) Ben Bitdiddle wants to use a one-time pad to send you messages, too, but he's lazy and doesn't want to make the one-time pad before sending his message.

"I know!" he says. "I'll just tell you a secret word – like CAT – and then use that secret word over and over and over again for my secret key, like CATCATCATCAT! That way, I never have to tell you any more letters, and we can always send encrypted messages!"

What is wrong with his proposal?

Below is a message that you intercept, sent from Ben Bitdiddle to Alyssa P. Hacker. It was not meant for your eyes, but you expect that you can guess the message, even though you don't know the secret word shared between Ben and Alyssa.

It was a two-letter word.

Encrypted Message –

AWEDHLAWKWFQYJBWGV

What is the message? What is the secret word?

Secret Word –

Decrypted Message –