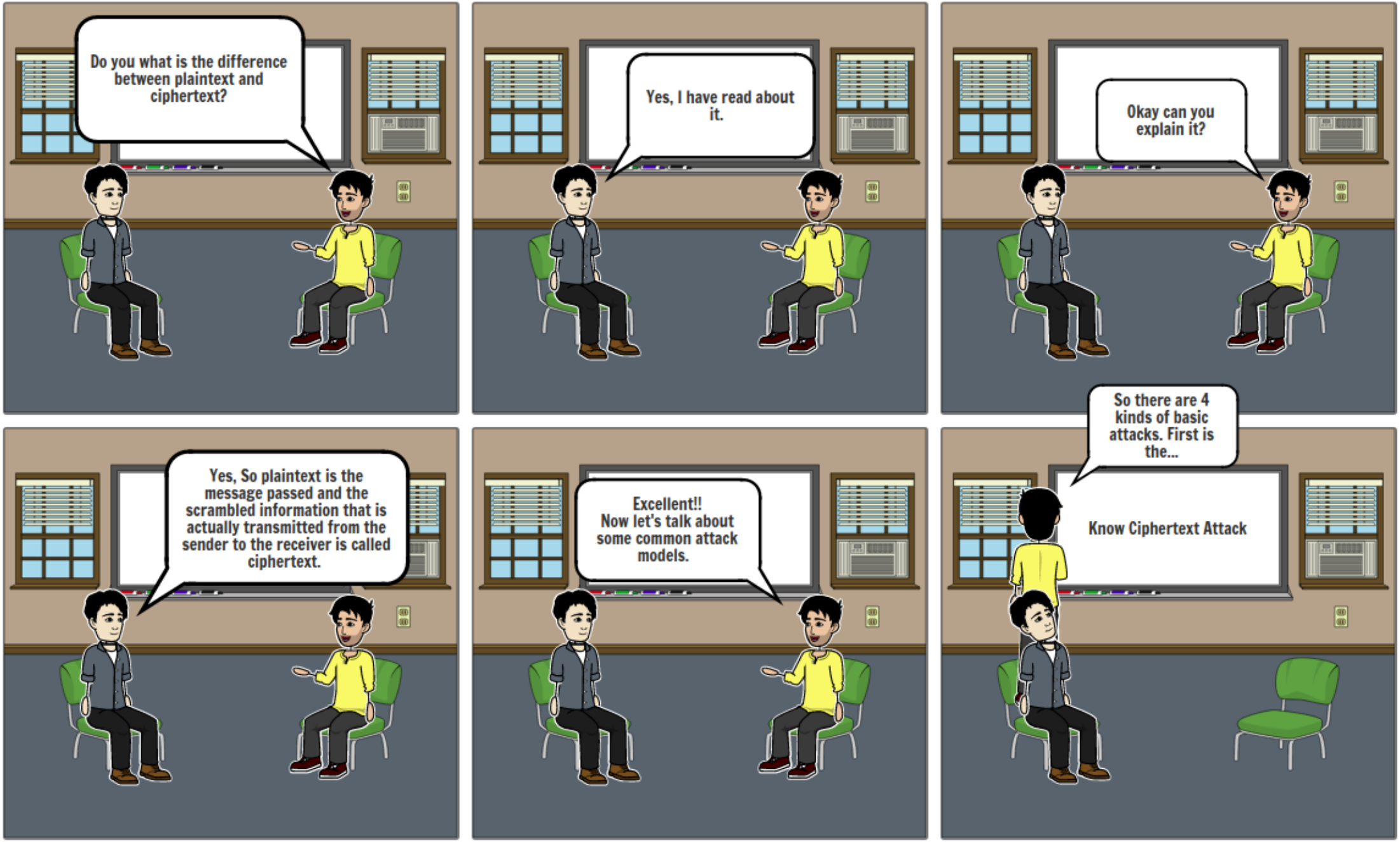
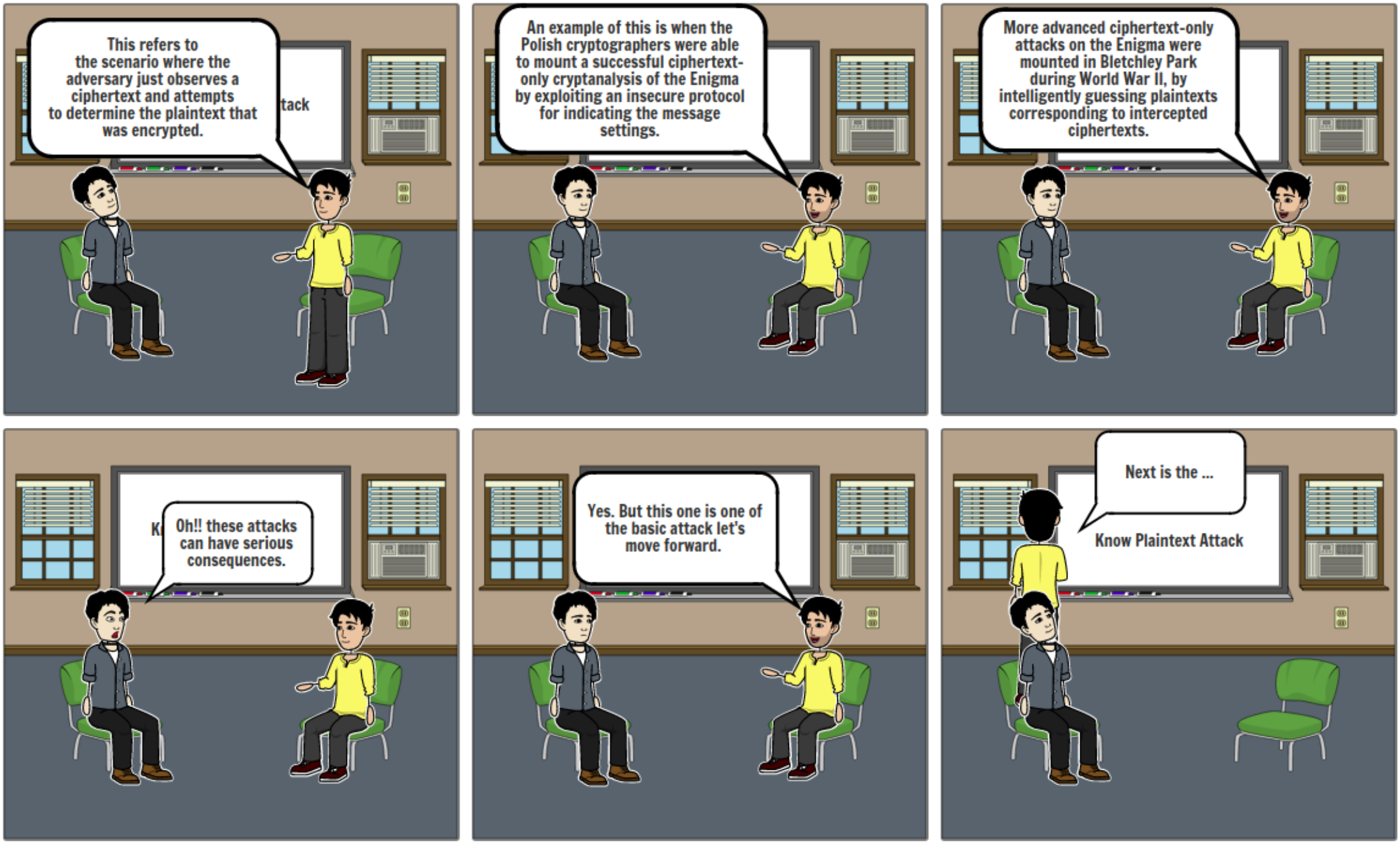
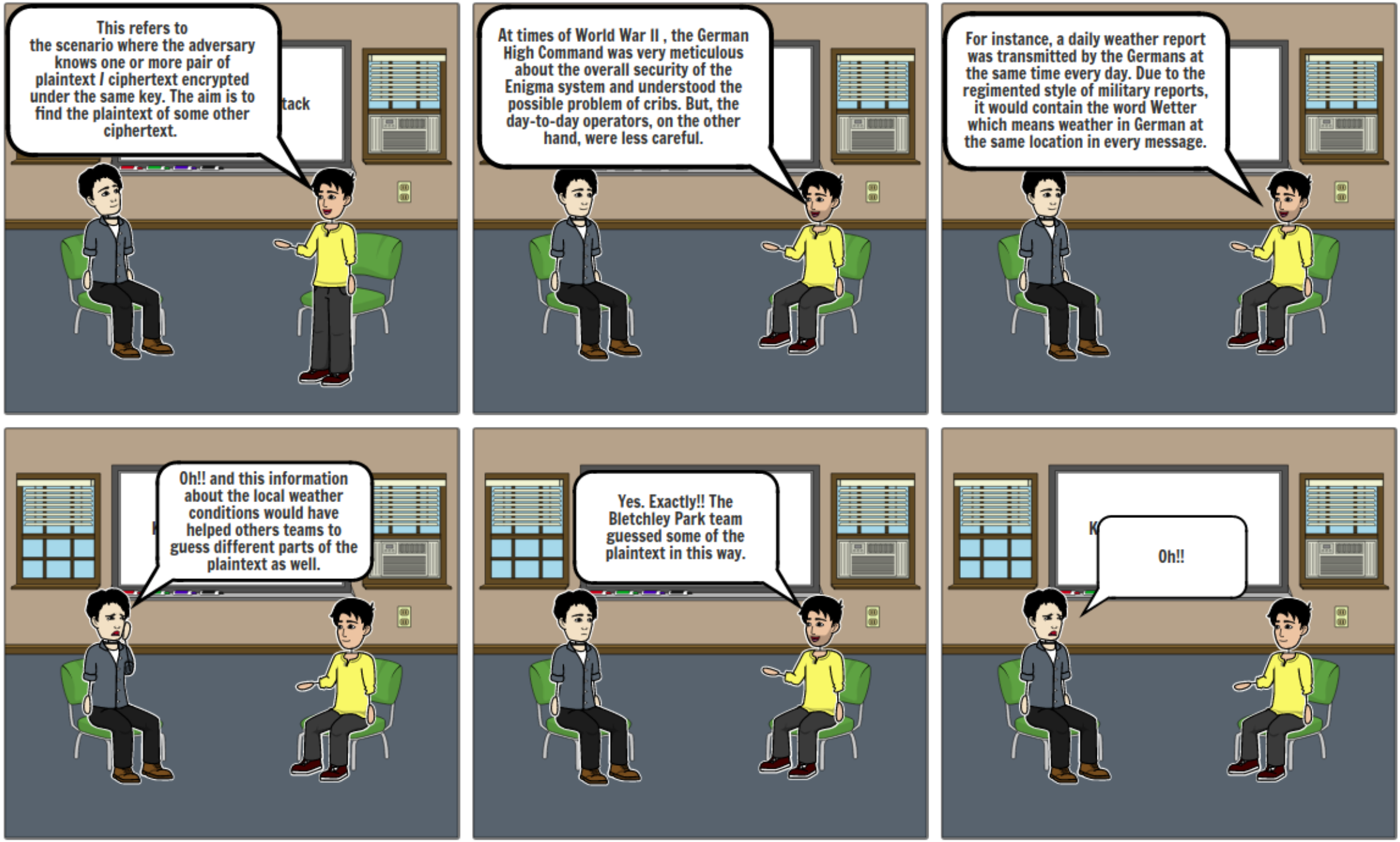
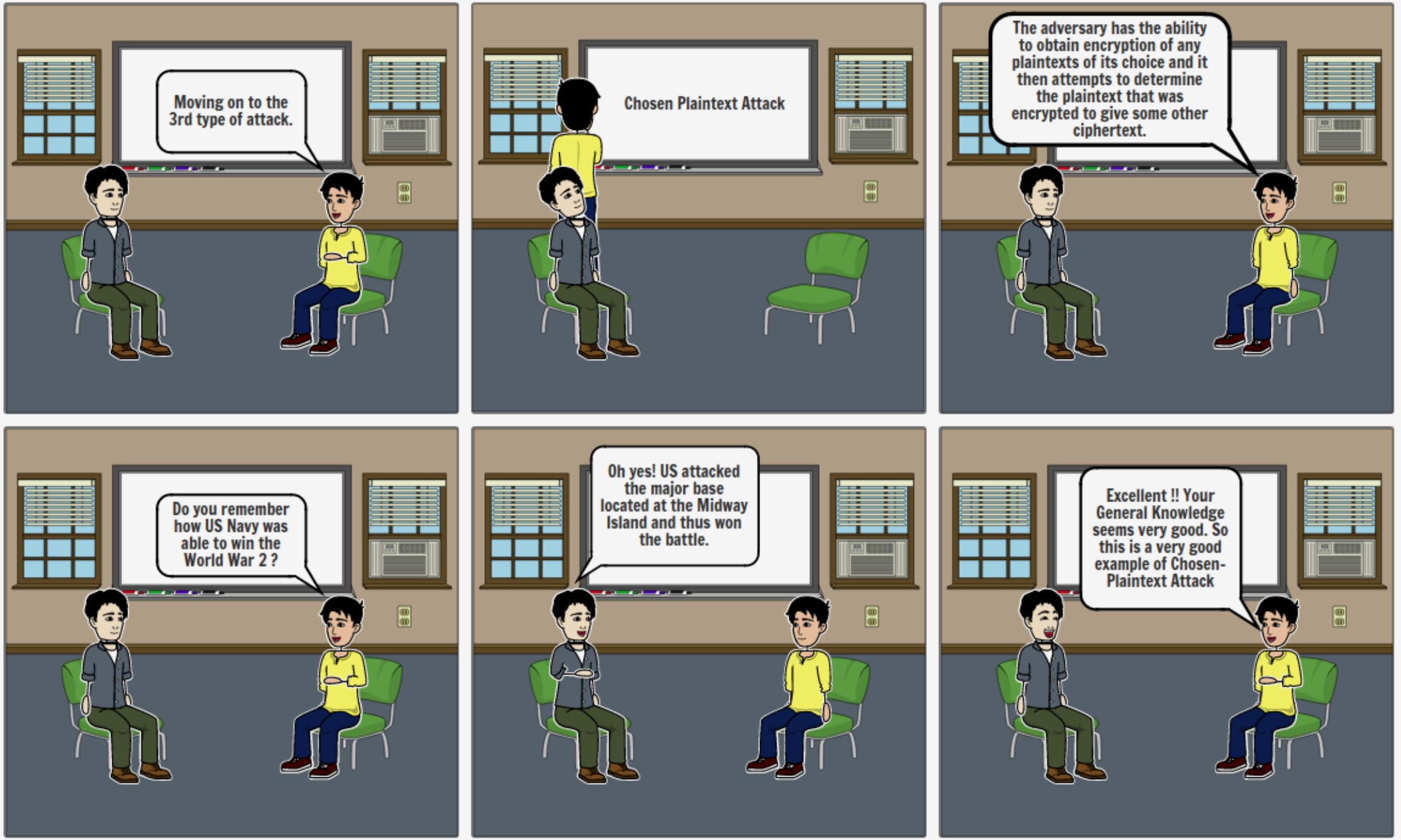
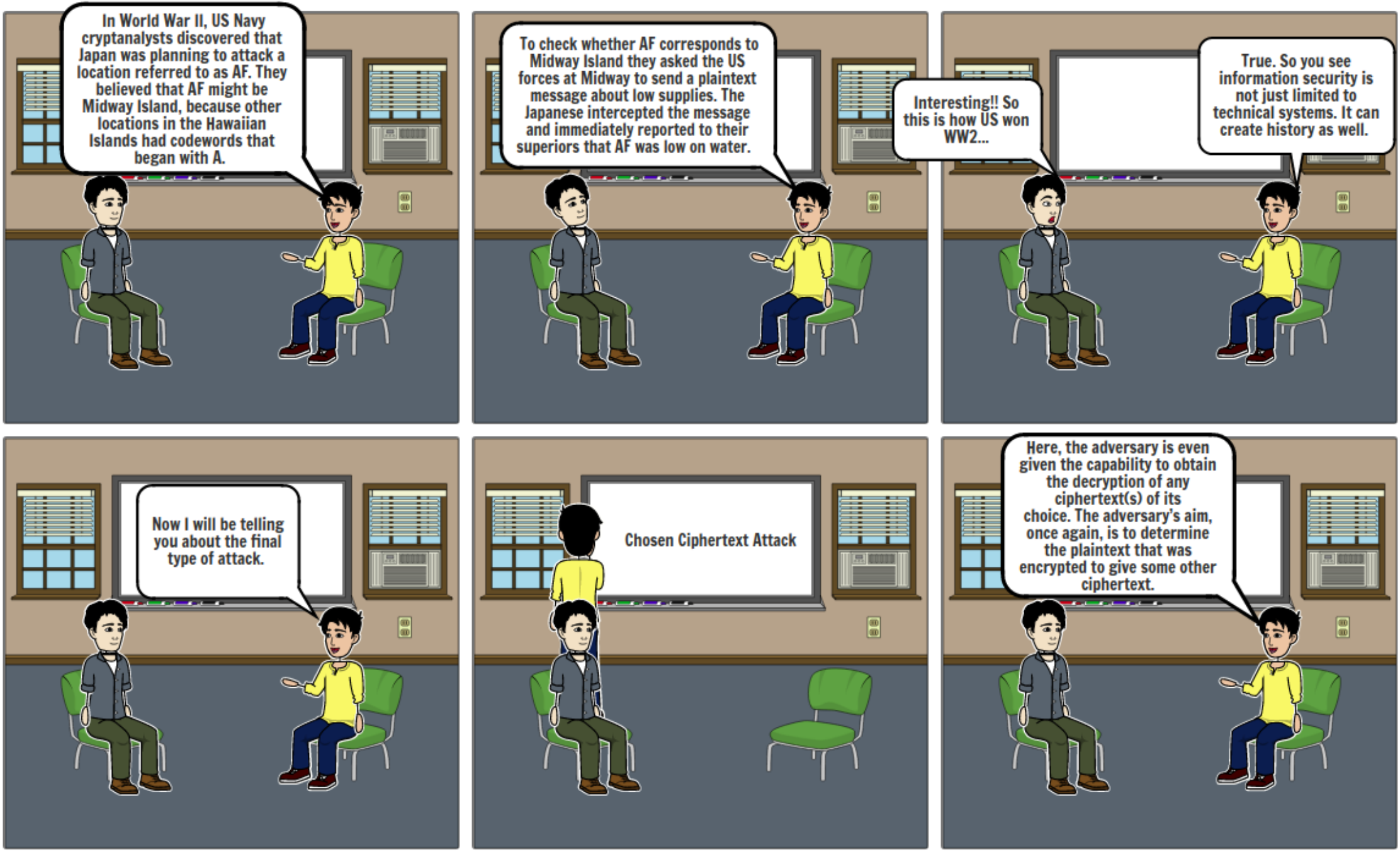
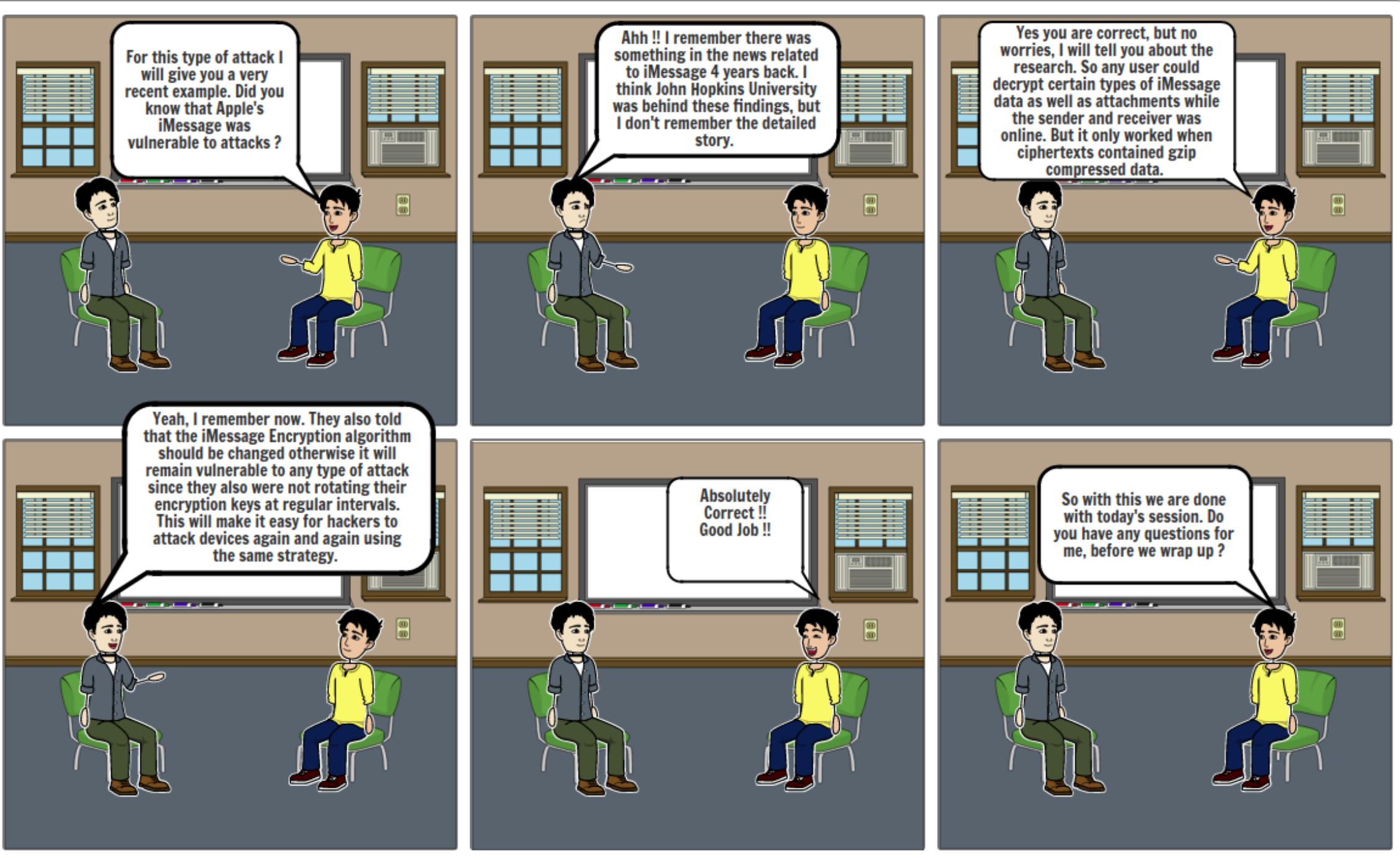

Do you what is the difference between plaintext and ciphertext?
Yes, I have read about it.
Okay can you explain it?
Yes, So plaintext is the message passed and the scrambled information that is actually transmitted from the sender to the receiver is called ciphertext.
Excellent!! Now let's talk about some common attack models.
So there are 4 kinds of basic attacks. First is the...
Know Ciphertext Attack

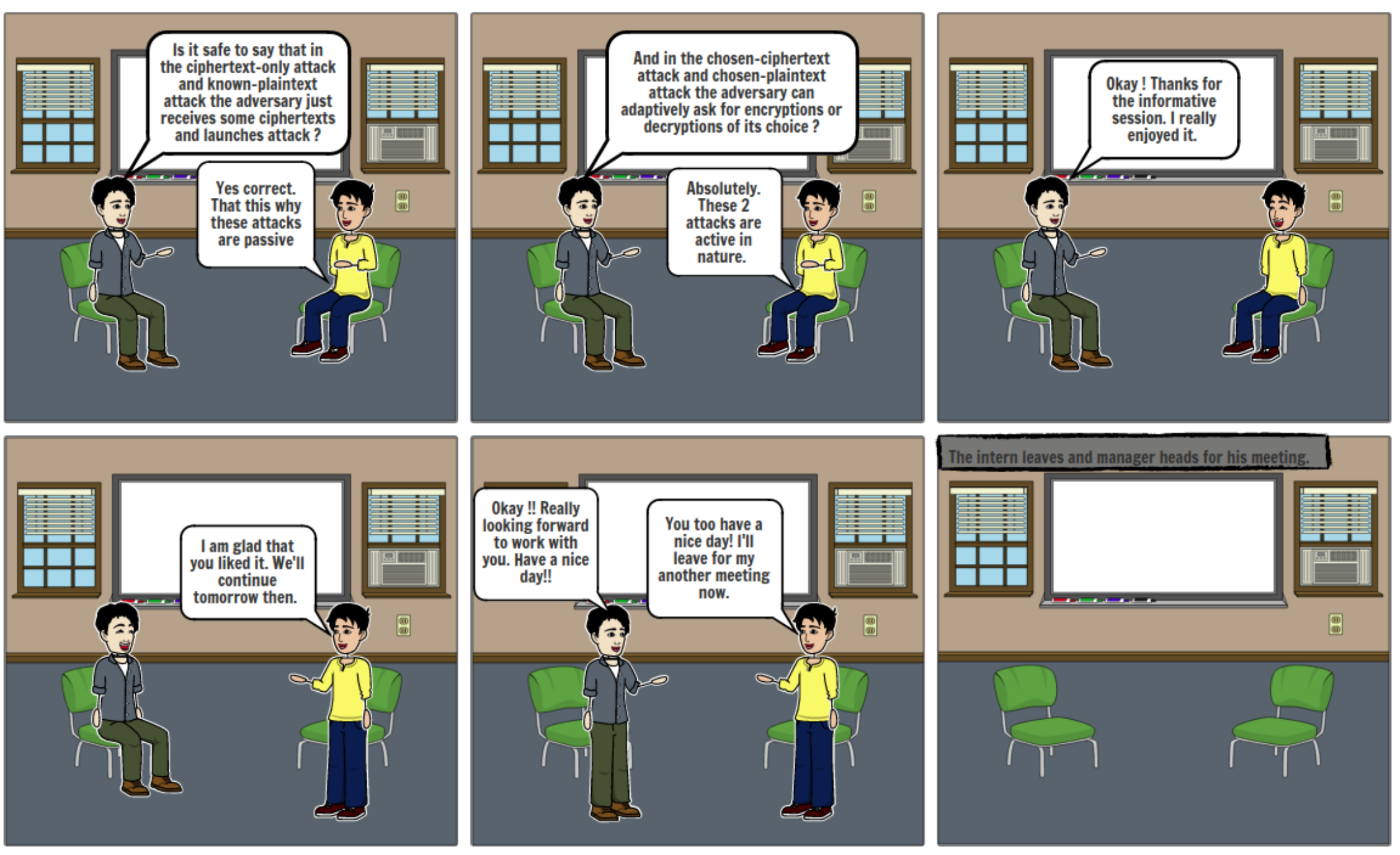

This refers to the scenario where the adversary just observes a ciphertext and attempts to determine the plaintext that was encrypted.
tack
An example of this is when the Polish cryptographers were able to mount a successful ciphertext-only cryptanalysis of the Enigma by exploiting an insecure protocol for indicating the message settings.
More advanced ciphertext-only attacks on the Enigma were mounted in Bletchley Park during World War II, by intelligently guessing plaintexts corresponding to intercepted ciphertexts.
K
Oh!! these attacks can have serious consequences.
Yes. But this one is one of the basic attack let's move forward.
Next is the ...
Know Plaintext Attack


This refers to the scenario where the adversary knows one or more pair of plaintext / ciphertext encrypted under the same key. The aim is to find the plaintext of some other ciphertext.
tack
At times of World War II , the German High Command was very meticulous about the overall security of the Enigma system and understood the possible problem of cribs. But, the day-to-day operators, on the other hand, were less careful.
For instance, a daily weather report was transmitted by the Germans at the same time every day. Due to the regimented style of military reports, it would contain the word Wetter which means weather in German at the same location in every message.
Oh!! and this information about the local weather conditions would have helped others teams to guess different parts of the plaintext as well.
Yes. Exactly!! The Bletchley Park team guessed some of the plaintext in this way.
Oh!!


Moving on to the 3rd type of attack.
Chosen Plaintext Attack
The adversary has the ability to obtain encryption of any plaintexts of its choice and it then attempts to determine the plaintext that was encrypted to give some other ciphertext.
Do you remember how US Navy was able to win the World War 2 ?
Oh yes! US attacked the major base located at the Midway Island and thus won the battle.
Excellent !! Your General Knowledge seems very good. So this is a very good example of Chosen-Plaintext Attack


In World War II, US Navy cryptanalysts discovered that Japan was planning to attack a location referred to as AF. They believed that AF might be Midway Island, because other locations in the Hawaiian Islands had codewords that began with A.
To check whether AF corresponds to Midway Island they asked the US forces at Midway to send a plaintext message about low supplies. The Japanese intercepted the message and immediately reported to their superiors that AF was low on water.
Interesting!! So this is how US won WW2...
True. So you see information security is not just limited to technical systems. It can create history as well.
Now I will be telling you about the final type of attack.
Chosen Ciphertext Attack
Here, the adversary is even given the capability to obtain the decryption of any ciphertext(s) of its choice. The adversary's aim, once again, is to determine the plaintext that was encrypted to give some other ciphertext.


For this type of attack I will give you a very recent example. Did you know that Apple's iMessage was vulnerable to attacks ?
Ahh !! I remember there was something in the news related to iMessage 4 years back. I think John Hopkins University was behind these findings, but I don't remember the detailed story.
Yes you are correct, but no worries, I will tell you about the research. So any user could decrypt certain types of iMessage data as well as attachments while the sender and receiver was online. But it only worked when ciphertexts contained gzip compressed data.
Yeah, I remember now. They also told that the iMessage Encryption algorithm should be changed otherwise it will remain vulnerable to any type of attack since they also were not rotating their encryption keys at regular intervals. This will make it easy for hackers to attack devices again and again using the same strategy.
Absolutely Correct !! Good Job !!
So with this we are done with today's session. Do you have any questions for me, before we wrap up ?


Is it safe to say that in the ciphertext-only attack and known-plaintext attack the adversary just receives some ciphertexts and launches attack ?
Yes correct. That this why these attacks are passive
And in the chosen-ciphertext attack and chosen-plaintext attack the adversary can adaptively ask for encryptions or decryptions of its choice ?
Absolutely. These 2 attacks are active in nature.
Okay ! Thanks for the informative session. I really enjoyed it.
I am glad that you liked it. We'll continue tomorrow then.
Okay !! Really looking forward to work with you. Have a nice day!!
You too have a nice day! I'll leave for my another meeting now.
The intern leaves and manager heads for his meeting.