Kyle Den Hartog
Homework 3
Computer Security
Problem 1:
Question 1:

1. A system secure against known plaintext attacks removes the need to keep past messages secret, which over time becomes more difficult as more messages are sent.
2. A system secure against chosen plaintext attacks prevents adversaries from creating false messages.
3. A system secure against chosen plaintext attacks also prevents an adversary from identifying information about the key to potentially break the system.

Question 2:

1. Requires the key to be shared in privately prior to communication which is not always a feasible option.

Question 3:

1. Message authentication can be repudiated (disputed) because both people can sign the message therefore it is not possible to identify which person created the message.

Question 4:

- A cryptosystem which is secure against a known plaintext attack (KPA) can be used to produce a one-way function (public key encryption)
    - If a cryptosystem is secure against a KPA than it can be assumed that one key can be distributed which allows for public key distribution
    - Given that an adversary would have access to a public key it is easy for a message to be encrypted with the public key, but difficult to compute the encrypted message without the private key an adversary would be unable to decrypt the message, but a person with the private key could easily. (property of a one-way function)
    - Therefore, it is a strong encryption system over public (unsecure) channels
- A public key cryptosystem can be used to generate a one-way authentication system (digital signature)
    - If User A encrypts a message using their private key, any person can use User A's public key to decrypt the message. It therefore be concluded that because the message has meaning, it can be concluded that only User A could have produced that message (given that User A keeps their private key secure)
- A trap-door cryptosystem (public key encryption) can be used to produce a public key distribution system
    - a trapdoor cryptosystem requires both keys to easily decrypt a message therefore, one key can be published creating a public key distribution system and the system is still considered secure.

Kyle Den Hartog
Homework 3
Computer Security

Problem 2:
Question 1:

- It depends upon the security level you set it the column to. For example, if you set it to RND or HOM security levels it is IND-CPA secure, but RND does not allow for computations to be done on the data and HOM requires a large amount of time to perform computations at this level making both infeasible options to databases that require a lot of changes to the database or its data. If you utilize lower security levels, the data can be still considered secure, but it is not IND-CPA secure. Therefore IND-CPA security is dependent on the security level implemented by the column.

Question 2:

- DTE requires an auxiliary dataset that is "well-correlated" with the plaintext column. Frequency analysis or l_p optimization attacks can then be coordinated with this information.

Question 3:

- No, it would not work if the attack is encrypted datasets are not dense enough. However, columns can still recover a large fraction of the column cells using a cumulative attack. This cumulative attack requires an additional dataset to compare ordering and frequencies against, so if the dataset is not great the attack becomes weaker. In other words, if your dataset contained only one element of data and the column using OPE was not dense enough, this attack would not work.