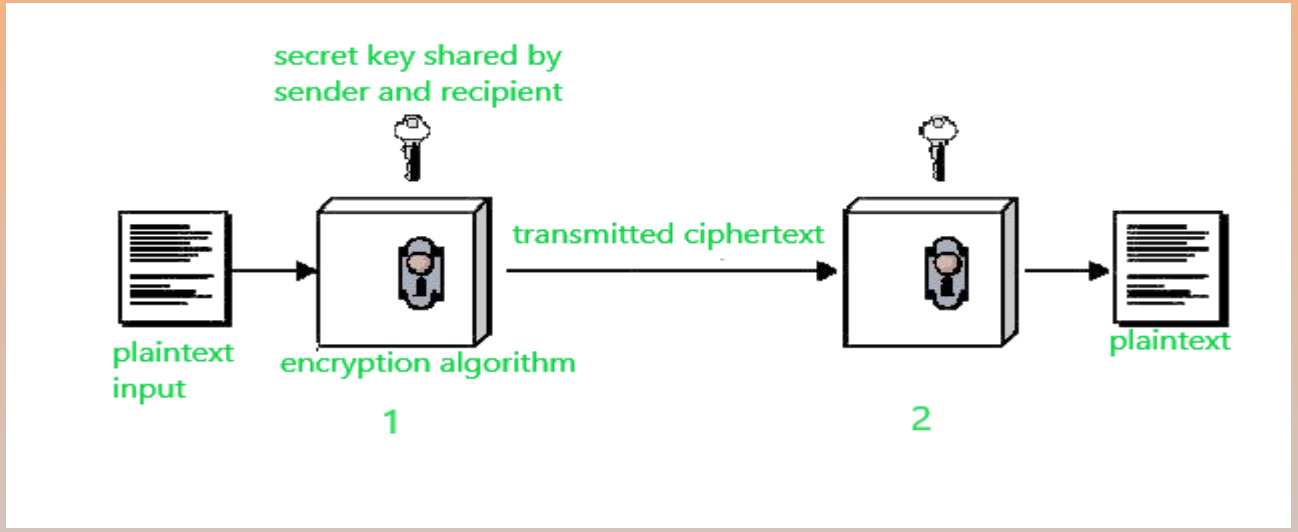
Cryptography and network security

By: Dr. Upma Jain

Conventional Encryption

- **Conventional encryption** is a cryptographic system that uses the same key.
- It is still much preferred of the two types of encryption systems due to its simplicity.
- It is a relatively fast process since it uses a single key for both encryption and decryption.
- In this encryption model, the sender encrypts plaintext using the receiver's secret key, which can be later used by the receiver to decrypt the ciphertext.



Conventional encryption has mainly 5 ingredients :

- **Plain text –** It is the original data that is given to the algorithm as an input.
- **Encryption algorithm –** This encryption algorithm performs various transformations on plain text to convert it into ciphertext.
- **Secret key –** The secret key is also an input to the algorithm. The encryption algorithm will produce different outputs based on the keys used at that time.
- **Ciphertext –** It contains encrypted information because it contains a form of original plaintext that is unreadable by a human or computer without proper cipher to decrypt it. It is output from the algorithm.
- **Decryption algorithm –** This is used to run encryption algorithms in reverse. Ciphertext and Secret key is input here and it produces plain text as output.

Requirements for secure use of conventional encryption:

- We need a strong encryption algorithm.
- The sender and Receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Advantages of Conventional Encryption :

- **Simple –**
  This type of encryption is easy to carry out.

- **Uses fewer computer resources –**
  Conventional encryption does not require a lot of computer resources when compared to public-key encryption.

- **Fast –**
  Conventional encryption is much faster than asymmetric key encryption.

Disadvantages of Conventional Encryption Model

- It isn’t much secured when compared to public-key encryption.
- If the receiver lost the key, he/she cant decrypt the message and thus making the whole process useless.
- This scheme does not scale well to a large number of users because both the sender and the receiver have to agree on a secret key before transmission.

Cryptanalysis

- Cryptography is the science and art of creating secret codes, **cryptanalysis** is the science of breaking those codes.
- Types of cryptanalysis attacks
  - Ciphertext only
  - Known Plaintext
  - Chosen Plaintext
  - Chosen Ciphertext

Ciphertext-Only

- In this, Eve has access to only **some ciphertext**. She tries to find the corresponding key and the plaintext.
- The **assumption** is that **Eve knows the algorithm** and can **intercept the ciphertext.**
- The ciphertext-only attack is the most probable one because Eve needs only the ciphertext for this attack.

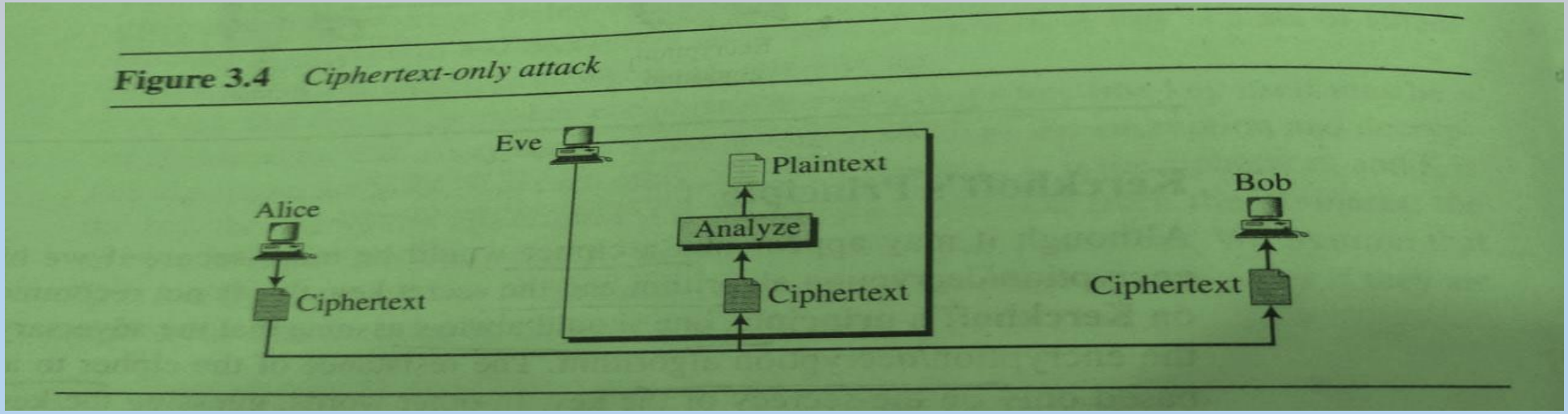


Fig. 2 Ciphertext only attack [Cryptography and network security (B.A. Forouzan]

Types of Ciphertext only attack

Various methods can be used in ciphertext-only attack.

- Brute-force
- Statistical Attack
- Pattern attack

Brute force attack

- We assume that Eve knows the algorithm and knows the key domain (all possible keys).
- Using the intercepted cipher, Eve decrypts the ciphertext with every possible key until the plaintext makes sense.
- Using brute-force attack was a difficult task in the past, it is easier today using a computer. To prevent this type of attack, the number of possible keys must be very large.

Statistical Attack

- The cryptanalyst can benefit from some inherent characteristics of the plaintext language to launch a statistical attack.
- For example, we know that the letter E is the most frequently used letter in English text. The cryptanalyst finds the mostly-used character in the ciphertext and assumes that the corresponding plaintext character is E.
- After finding a few pairs, the analyst can find the key and use it to decrypt the message. To prevent this type of attack, the cipher should hide the characteristics of the language.

Pattern attack

- Some ciphers may hide the characteristics of the language, but may create some patterns in the ciphertext.
- A cryptanalyst may use a pattern attack to break the cipher Therefore, it is important to use ciphers that make the ciphertext look as random as possible.

Known-Plaintext Attack

- In this, Eve has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext that she wants to break, as shown in Figure.

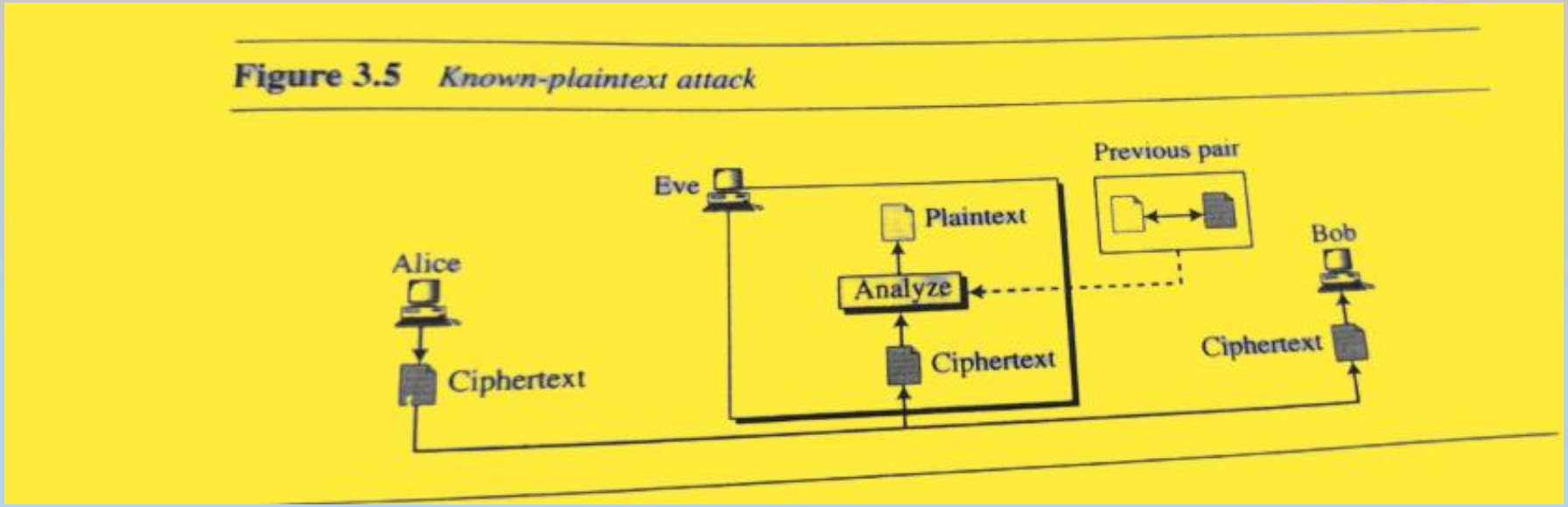


Fig. 3 Known Plaintext attack [Cryptography and network security (B.A. Forouzan]

- The plaintext/ciphertext pairs have been collected earlier. For example, Alice has sent a secret message to Bob, but she has later made the contents of the message public.
- Eve has kept both the ciphertext and the plaintext to use them to break the next secret message from Alice to Bob, assuming that Alice has not changed her key.
- Eve uses the relationship between the previous pair to analyze the current ciphertext.
- The same methods used in a ciphertext-only attack can be applied here.
- This attack is easier to implement because Eve has more information to use for analysis. However, it is less likely to happen because Alice may have changed her key or may have not disclosed the contents of any previous messages.

Chosen-plaintext Attack

- The chosen-plaintext attack is similar to the known-plaintext attack, but the plaintext/ ciphertext pairs have been chosen by the attacker herself.

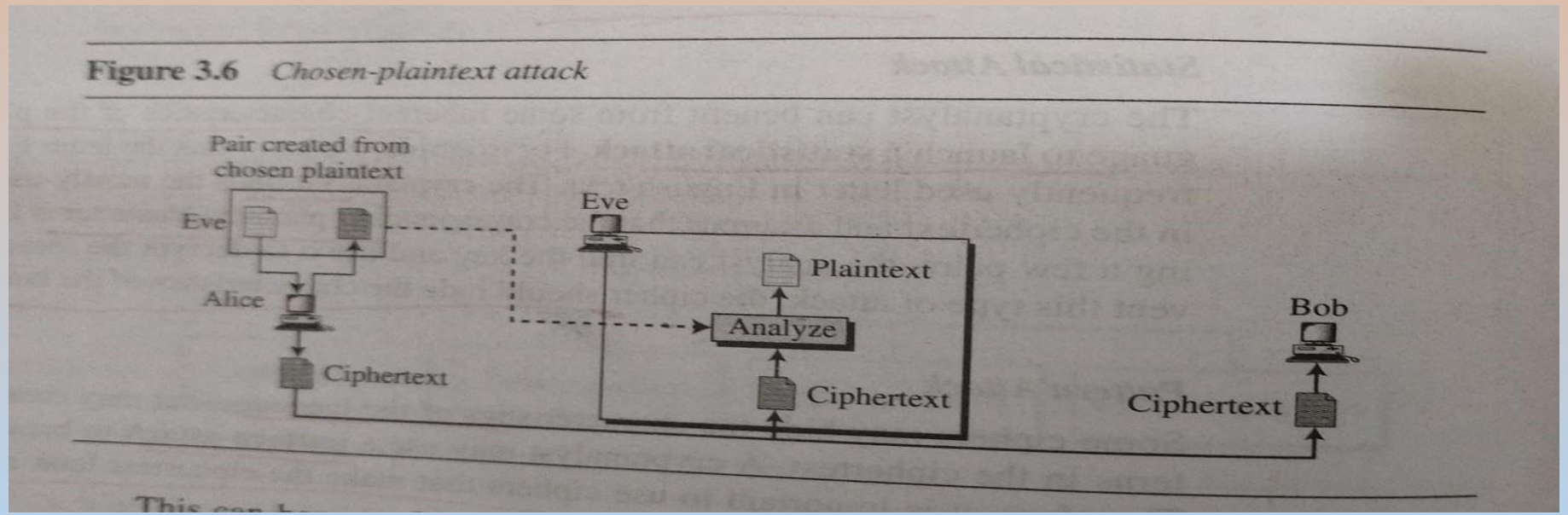


Fig. 4 Ciphertext only attack [Cryptography and network security (B.A. Forouzan]

- This can happen, for example, if Eve has access to Alice's computer. She can choose some plaintext and intercept the created ciphertext. Of course, she does not have the key because the key is normally embedded in the software used by the sender. This type of attack is much easier to implement, but it is much less likely to happen.

Chosen-Ciphertext Attack

The chosen-ciphertext attack is similar to the chosen-plaintext attack, except that Eve chooses some ciphertext and decrypts it to form a ciphertext/plaintext pair. This can happen if Eve has access to Bob's computer. Figure shows the process.

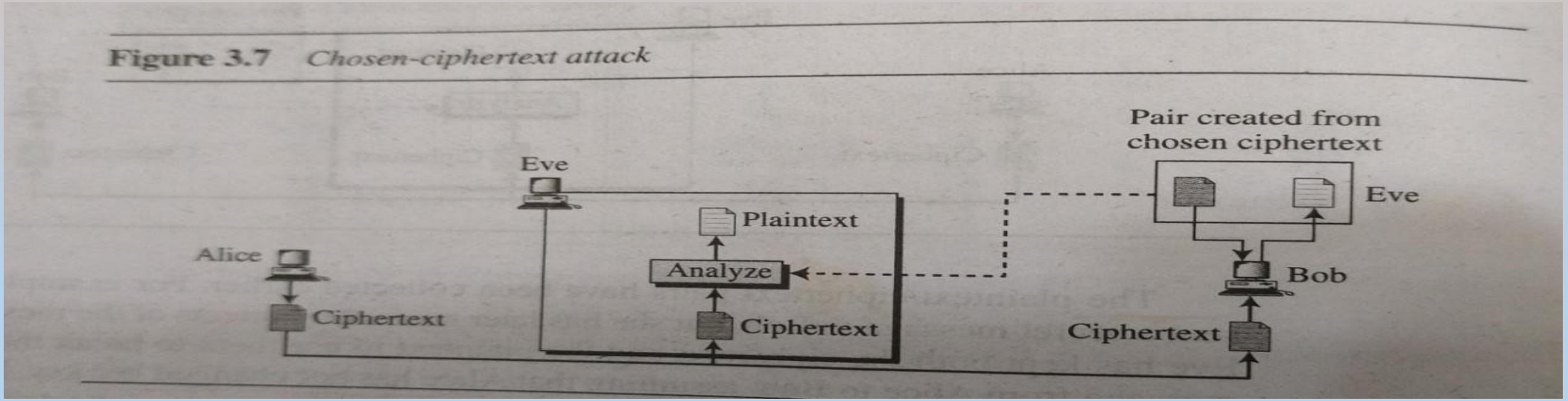


Fig. 5 Chosen- Ciphertext attack [Cryptography and network security (B.A. Forouzan)]

Thank You