**Symmetric Encryption**

- **Video:** Cryptography
  7 min
- **Reading:** Supplemental Reading for The Future of Cryptanalysis
  10 min
- **Video:** Symmetric Cryptography
  4 min
- **Video:** Symmetric Encryption Algorithms
  7 min
- **Reading:** Supplemental Reading for Symmetric Encryptions
  10 min
- **Practice Quiz:** Symmetric Encryption
  5 questions
- **Video:** Rob: The work of a security engineer
  1 min

**Public Key or Asymmetric Encryption**

**Hashing**

**Cryptography Applications**

**Graded Assessments**

# Supplemental Reading for The Future of Cryptanalysis

## The Future of Cryptanalysis

Data security is one of the top issues for companies. Being familiar with how data is protected and the attacks that can occur within a company to get sensitive information is a crucial aspect of an IT professionals role. This reading covers the definitions of cryptography and cryptanalysis as well as the five types of attacks and their outcomes.

### Cryptography

Cryptography is a method of protecting information and communications using codes so that only the intended person can read and process them. Cryptography has mainly stemmed from the manual encoding of messages and information using a formula to convert any given letter or number to a new value. Encryption is the process that encodes the data making it harder to decode. The goal of encrypting data is to keep internal information secure.

### Cryptanalysis

Cryptanalysis uses technology to improve the process of encrypting data and innovates new ways to defend companies from attacks that can access and decode their data.

## Impact of technology

Many modern encryption algorithms are based on large prime number factorization. This factorization is difficult to do by hand since there are millions of options for these algorithms. Once the information has been encrypted using the algorithm, it is called ciphertext. Technology has evolved to create harder algorithms but also makes it easier to crack algorithms. Modern quantum computers can crack encryption keys significantly faster using factorization and brute-force attacks. An encryption key is typically a random string of bits generated specifically to scramble and unscramble data. The encryption key is then used to convert the ciphertext to plaintext, which is not encoded.

## Types of cryptanalysis attack

There are several types of attacks that hackers or security professionals employ to get data from a network using cryptanalysis. The attacks all use a different way into the network to gain encoded information and translate it from the encoded form into information that can be easily read.

The following are the most common cryptanalytic attacks:

- **Known-Plaintext Analysis (KPA)** requires access to some or all of the plaintext of the encrypted information. The plaintext is not computationally tagged, specially formatted, or written in code. The analyst's goal is to examine the known plaintext to determine the key used to encrypt the message. Then they use the  key to decrypt the encoded information.
- **Chosen-Plaintext Analysis (CPA)** requires that the attacker knows the encryption algorithm or has access to the device used to do the encryption. The analyst can encrypt one block of chosen plaintext with the targeted algorithm to get information about the key. Once the analyst obtains the key, they can decrypt and use sensitive information.
- **Ciphertext-Only Analysis (COA)** requires access to one or more encrypted messages. No information is needed about the plaintext data, the algorithm, or data about the cryptographic key. Intelligence agencies face this challenge when intercepting encrypted communications with no key.
- **Adaptive Chosen-Plaintext Attack (ACPA)** is similar to a chosen-plaintext attack. Unlike a CPA, it can use smaller lines of plaintext to receive its encrypted ciphertext and then crack the encryption code using the ciphertext.
- **Meddler-in-the-Middle (MITM)** uses cryptanalysts to insert a meddler between two communication devices or applications to exchange their keys for secure communication. The meddler replies as the user and then performs a key exchange with each party. The users or systems think they communicate with each other, not the meddler. These attacks allow the meddler to obtain login credentials and other sensitive information.

## Results from a cryptanalysis attack

There are various results of a cryptanalysis attack. Some attacks result in a total break in the encryption and some result in more information that can help the attacker cause other damage or get closer to the goal of a total break.

Common results from a cryptanalysis attack include:

- **Instance deduction** where the attacker discovers additional plain or cipher text. While the key isn't found to break the code, the additional plaintext or ciphertext can be used to cause problems or continue attacks.
- **Information deduction** where the attacker obtains some information about plain or cipher text not previously known. The additional information can lead to more information about the encryption key.
- **Distinguishing algorithm** where the attacker can distinguish the encryption algorithm from a random alteration. This information reveals clues about the encryption algorithm and can lead to more significant breaks.
- **Global deduction** where the attacker finds an algorithm that is functionally equivalent to the one used in the key. This algorithm is then used to decrypt all information and messages.
- **Total break** where the attacker can gain the entire key. With the entire key, the attacker can decrypt all messages and information.

## Key takeaways

Many companies use encryption to protect the sensitive information on their network

- Technology has advanced cryptanalysis, using more complex algorithms to encrypt data. Modern quantum computers also make it easier to use cryptanalysis to break a company's encryption.
- The different types of attacks that focus on plaintext and ciphertext are Known-Plaintext Analysis, Chosen-Plaintext Analysis, Ciphertext-Only Analysis, and Adaptive Chosen-Plaintext Attack. The meddler in the middle attack is another cryptanalysis attack that gets the key from intercepting a key exchange.
- There are various results of a cryptanalysis attack including Instance deduction, Information deduction, Distinguishing algorithm, Global deduction, and Total break.

## More resources

- To learn more about the history of cryptanalysis, see this Wikipedia article on Cryptanalysis.
- For more information on large prime number factorization, see Integer Factorization.
- To read more about cryptanalysis techniques and attacks, see Cryptanalysis explained.

**Mark as completed**

**Like** **Dislike** **Report an issue**