Name : ايمان سيد صبري سيد

ID : 230

Group: 2

Sec:10

* Cryptography system 5 webpage

1. Home

<div id="home">

            <p>Before the modern era, cryptography focused on message confidentiality (i.e., encryption)—conversion of

                messages from a comprehensible form into an incomprehensible one and back again at the other end,

                rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed

                for decryption of that message). Encryption attempted to ensure secrecy in communications, such as those

                of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond

                confidentiality concerns to include techniques for message integrity checking, sender/receiver identity

                authentication, digital signatures, interactive proofs and secure computation, among others.

            </p>

        </div>

1. Classification

<div id="classification">

            <table>

                <caption>classification of cryptography</caption>

                <tr>

                    <th scope="col">cryptography </th>

                </tr>

                <tr>

                    <td>symmetric key </td>

                </tr>

                <tr>

                    <td>Asymmetric key</td>

                </tr>

                <tr>

                    <td>Hash function</td>

                </tr>

            </table>

        </div>

1. cryptanalysis

 <div id="Cryptanalysis">

            <p>

                The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus

                permitting its subversion or evasion.

                It is a common misconception that every encryption method can be broken. In connection with his WWII

                work at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key

                material is truly random, never reused, kept secret from all possible attackers, and of equal or greater

                length than the message.[50] Most ciphers, apart from the one-time pad, can be broken with enough

                computational effort by brute force attack, but the amount of effort needed may be exponentially

                dependent on the key size, as compared to the effort needed to make use of the cipher. In such cases,

                effective security could be achieved if it is proven that the effort required (i.e., "work factor", in

                Shannon's terms) is beyond the ability of any adversary. This means it must be shown that no efficient

                method (as opposed to the time-consuming brute force method) can be found to break the cipher. Since no

                such proof has been found to date, the one-time-pad remains the only theoretically unbreakable cipher.

                Although well-implemented one-time-pad encryption cannot be broken, traffic analysis is still possible.

                There are a wide variety of cryptanalytic attacks, and they can be classified in any of several ways. A

                common distinction turns on what Eve (an attacker) knows and what capabilities are available. In a

                ciphertext-only attack, Eve has access only to the ciphertext (good modern cryptosystems are usually

                effectively immune to ciphertext-only attacks). In a known-plaintext attack, Eve has access to a

                ciphertext and its corresponding plaintext (or to many such pairs). In a chosen-plaintext attack, Eve

                may choose a plaintext and learn its corresponding ciphertext (perhaps many times); an example is

                gardening, used by the British during WWII. In a chosen-ciphertext attack, Eve may be able to choose

                ciphertexts and learn their corresponding plaintexts.[4] Finally in a man-in-the-middle attack Eve gets

                in between Alice (the sender) and Bob (the recipient), accesses and modifies the traffic and then

                forwards it to the recipient.[51] Also important, often overwhelmingly so, are mistakes (generally in

                the design or use of one of the protocols involved).

            </p>

        </div>

1. Lightweight cryptography

 <div id="Lightweight cryptography">

            Lightweight cryptography (LWC) concerns cryptographic algorithms developed for a strictly constrained

            environment. The growth of Internet of Things (IoT) has spiked research into the development of lightweight

            algorithms that are better suited for the environment. An IoT environment requires strict constraints on

            power consumption, processing power, and security.[59] Algorithms such as PRESENT, AES, and SPECK are

            examples of the many LWC algorithms that have been developed to achieve the standard set by the National

            Institute of Standards and Technology.

            <!-- img of NSA involvement -->

            <img

                src="data:image/png;base64,">

        </div>

1. prohibitions

<div id="Prohibitions">

            Cryptography has long been of interest to intelligence gathering and law enforcement agencies.[8] Secret

            communications may be criminal or even treasonous[citation needed]. Because of its facilitation of privacy,

            and the diminution of privacy attendant on its prohibition, cryptography is also of considerable interest to

            civil rights supporters. Accordingly, there has been a history of controversial legal issues surrounding

            cryptography, especially since the advent of inexpensive computers has made widespread access to

            high-quality cryptography possible.

            In some countries, even the domestic use of cryptography is, or has been, restricted. Until 1999, France

            significantly restricted the use of cryptography domestically, though it has since relaxed many of these

            rules. In China and Iran, a license is still required to use cryptography.[6] Many countries have tight

            restrictions on the use of cryptography. Among the more restrictive are laws in Belarus, Kazakhstan,

            Mongolia, Pakistan, Singapore, Tunisia, and Vietnam.

            In the United States, cryptography is legal for domestic use, but there has been much conflict over legal

            issues related to cryptography.[8] One particularly important issue has been the export of cryptography and

            cryptographic software and hardware. Probably because of the importance of cryptanalysis in World War II and

            an expectation that cryptography would continue to be important for national security, many Western

            governments have, at some point, strictly regulated export of cryptography. After World War II, it was

            illegal in the US to sell or distribute encryption technology overseas; in fact, encryption was designated

            as auxiliary military equipment and put on the United States Munitions List.[62] Until the development of

            the personal computer, asymmetric key algorithms (i.e., public key techniques), and the Internet, this was

            not especially problematic. However, as the Internet grew and computers became more widely available,

            high-quality encryption techniques became well known around the globe.

        </div>

* The full html project

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <!-- font awsome -->

    <title>cryptogrphy</title>

</head>

<body>

    <header>

        <p class="logo">cryptogrphy</p>

        <!-- list of anchor -->

        <ul>

            <li><a href="#home">home</a> </li>

            <li><a href="#classification">classification</a></li>

            <li><a href="#Cryptanalysis">Cryptanalysis</a></li>

            <li><a href="#Lightweight cryptography">Lightweight cryptography</a></li>

            <li><a href="#Prohibitions">Prohibitions</a></li>

        </ul>

    </header>

    <main>

        <div id="home">

            <p>Before the modern era, cryptography focused on message confidentiality (i.e., encryption)—conversion of

                messages from a comprehensible form into an incomprehensible one and back again at the other end,

                rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed

                for decryption of that message). Encryption attempted to ensure secrecy in communications, such as those

                of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond

                confidentiality concerns to include techniques for message integrity checking, sender/receiver identity

                authentication, digital signatures, interactive proofs and secure computation, among others.

            </p>

        </div>

        <!-- table for cryptogrphy   -->

        <div id="classification">

            <table>

                <caption>classification of cryptography</caption>

                <tr>

                    <th scope="col">cryptography </th>

                </tr>

                <tr>

                    <td>symmetric key </td>

                </tr>

                <tr>

                    <td>Asymmetric key</td>

                </tr>

                <tr>

                    <td>Hash function</td>

                </tr>

            </table>

        </div>

        <div id="Cryptanalysis">

            <p>

                The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus

                permitting its subversion or evasion.

                It is a common misconception that every encryption method can be broken. In connection with his WWII

                work at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key

                material is truly random, never reused, kept secret from all possible attackers, and of equal or greater

                length than the message.[50] Most ciphers, apart from the one-time pad, can be broken with enough

                computational effort by brute force attack, but the amount of effort needed may be exponentially

                dependent on the key size, as compared to the effort needed to make use of the cipher. In such cases,

                effective security could be achieved if it is proven that the effort required (i.e., "work factor", in

                Shannon's terms) is beyond the ability of any adversary. This means it must be shown that no efficient

                method (as opposed to the time-consuming brute force method) can be found to break the cipher. Since no

                such proof has been found to date, the one-time-pad remains the only theoretically unbreakable cipher.

                Although well-implemented one-time-pad encryption cannot be broken, traffic analysis is still possible.

                There are a wide variety of cryptanalytic attacks, and they can be classified in any of several ways. A

                common distinction turns on what Eve (an attacker) knows and what capabilities are available. In a

                ciphertext-only attack, Eve has access only to the ciphertext (good modern cryptosystems are usually

                effectively immune to ciphertext-only attacks). In a known-plaintext attack, Eve has access to a

                ciphertext and its corresponding plaintext (or to many such pairs). In a chosen-plaintext attack, Eve

                may choose a plaintext and learn its corresponding ciphertext (perhaps many times); an example is

                gardening, used by the British during WWII. In a chosen-ciphertext attack, Eve may be able to choose

                ciphertexts and learn their corresponding plaintexts.[4] Finally in a man-in-the-middle attack Eve gets

                in between Alice (the sender) and Bob (the recipient), accesses and modifies the traffic and then

                forwards it to the recipient.[51] Also important, often overwhelmingly so, are mistakes (generally in

                the design or use of one of the protocols involved).

            </p>

        </div>

        <div id="Lightweight cryptography">

            Lightweight cryptography (LWC) concerns cryptographic algorithms developed for a strictly constrained

            environment. The growth of Internet of Things (IoT) has spiked research into the development of lightweight

            algorithms that are better suited for the environment. An IoT environment requires strict constraints on

            power consumption, processing power, and security.[59] Algorithms such as PRESENT, AES, and SPECK are

            examples of the many LWC algorithms that have been developed to achieve the standard set by the National

            Institute of Standards and Technology.

            <!-- img of NSA involvement -->

            <img

                src="data:image/png;base64,">

        </div>

        <div id="Prohibitions">

            Cryptography has long been of interest to intelligence gathering and law enforcement agencies.[8] Secret

            communications may be criminal or even treasonous[citation needed]. Because of its facilitation of privacy,

            and the diminution of privacy attendant on its prohibition, cryptography is also of considerable interest to

            civil rights supporters. Accordingly, there has been a history of controversial legal issues surrounding

            cryptography, especially since the advent of inexpensive computers has made widespread access to

            high-quality cryptography possible.

            In some countries, even the domestic use of cryptography is, or has been, restricted. Until 1999, France

            significantly restricted the use of cryptography domestically, though it has since relaxed many of these

            rules. In China and Iran, a license is still required to use cryptography.[6] Many countries have tight

            restrictions on the use of cryptography. Among the more restrictive are laws in Belarus, Kazakhstan,

            Mongolia, Pakistan, Singapore, Tunisia, and Vietnam.

            In the United States, cryptography is legal for domestic use, but there has been much conflict over legal

            issues related to cryptography.[8] One particularly important issue has been the export of cryptography and

            cryptographic software and hardware. Probably because of the importance of cryptanalysis in World War II and

            an expectation that cryptography would continue to be important for national security, many Western

            governments have, at some point, strictly regulated export of cryptography. After World War II, it was

            illegal in the US to sell or distribute encryption technology overseas; in fact, encryption was designated

            as auxiliary military equipment and put on the United States Munitions List.[62] Until the development of

            the personal computer, asymmetric key algorithms (i.e., public key techniques), and the Internet, this was

            not especially problematic. However, as the Internet grew and computers became more widely available,

            high-quality encryption techniques became well known around the globe.

        </div>

    </main>

</body>

</html>