Name : محمود ابراهيم محمود ابراهيم

ID : 838

Group: 7

Sec: 38

* Cryptography system

1. Home

        <div id="home">

            <p>

                The first use of the term cryptograph (as opposed to cryptogram) dates back to the 19th

                century—originating from The Gold-Bug, a story by Edgar Allan Poe.[10][11][broken footnote]

                Until modern times, cryptography referred almost exclusively to encryption, which is the process of

                converting ordinary information (called plaintext) into unintelligible form (called ciphertext).[12]

                Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.

                A cipher (or cypher) is a pair of algorithms that carry out the encryption and the reversing decryption.

                The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a

                "key". The key is a secret (ideally known only to the communicants), usually a string of characters

                (ideally short so it can be remembered by the user), which is needed to decrypt the ciphertext. In

                formal mathematical terms, a "cryptosystem" is the ordered list of elements of finite possible

                plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption

                algorithms which correspond to each key. Keys are important both formally and in actual practice, as

                ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are

                therefore useless (or even counter-productive) for most purposes.

                Historically, ciphers were often used directly for encryption or decryption without additional

                procedures such as authentication or integrity checks. There are, generally, two kinds of cryptosystems:

                symmetric and asymmetric. In symmetric systems, the only ones known until the 1970s, the same key (the

                secret key) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster

                than asymmetric systems in part because they generally use shorter key lengths. Asymmetric systems use a

                "public key" to encrypt a message and a related "private key" to decrypt it. The use of asymmetric

                systems enhances the security of communication, largely because the relation between the two keys is

                very hard to discover.[13] Examples of asymmetric systems include RSA (Rivest–Shamir–Adleman), and ECC

                (Elliptic Curve Cryptography). Quality symmetric algorithms include the commonly used AES (Advanced

                Encryption Standard) which replaced the older DES (Data Encryption Standard).[14] Not very high quality

                symmetric algorithms include the assorted children's language tangling schemes such as Pig Latin or

                other cant, and indeed effectively all cryptographic schemes, however seriously intended, from any

                source prior to the invention of the one-time pad early in the 20th century.

                In colloquial use, the term "code" is often used to mean any method of encryption or concealment of

                meaning. However, in cryptography, code has a more specific meaning: the replacement of a unit of

                plaintext (i.e., a meaningful word or phrase) with a code word (for example, "wallaby" replaces "attack

                at dawn"). A cypher, in contrast, is a scheme for changing or substituting an element below such a level

                (a letter, or a syllable or a pair of letters or ...) in order to produce a cyphertext.

                Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted

                information without access to the key normally required to do so; i.e., it is the study of how to

                "crack" encryption algorithms or their implementations.

                Some use the terms cryptography and cryptology interchangeably in English, while others (including US

                military practice generally) use cryptography to refer specifically to the use and practice of

                cryptographic techniques and cryptology to refer to the combined study of cryptography and

                cryptanalysis.[15][16] English is more flexible than several other languages in which cryptology (done

                by cryptologists) is always used in the second sense above. RFC 2828 advises that steganography is

                sometimes included in cryptology.[17]

                The study of characteristics of languages that have some application in cryptography or cryptology (e.g.

                frequency data, letter combinations, universal patterns, etc.) is called cryptolinguistics.

            </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. Modren cryptography

        <div id="modren cryptography">

            <p>

                Cryptanalysis of the new mechanical devices proved to be both difficult and laborious. In the United

                Kingdom, cryptanalytic efforts at Bletchley Park during WWII spurred the development of more efficient

                means for carrying out repetitious tasks. This culminated in the development of the Colossus, the

                world's first fully electronic, digital, programmable computer, which assisted in the decryption of

                ciphers generated by the German Army's Lorenz SZ40/42 machine.

                Extensive open academic research into cryptography is relatively recent; it began only in the mid-1970s.

                In recent times, IBM personnel designed the algorithm that became the Federal (i.e., US) Data Encryption

                Standard; Whitfield Diffie and Martin Hellman published their key agreement algorithm;[31] and the RSA

                algorithm was published in Martin Gardner's Scientific American column. Since then, cryptography has

                become a widely used tool in communications, computer networks, and computer security generally.

                Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems

                are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep

                connections with abstract mathematics. There are very few cryptosystems that are proven to be

                unconditionally secure. The one-time pad is one, and was proven to be so by Claude Shannon. There are a

                few important algorithms that have been proven secure under certain assumptions. For example, the

                infeasibility of factoring extremely large integers is the basis for believing that RSA is secure, and

                some other systems, but even so, proof of unbreakability is unavailable since the underlying

                mathematical problem remains open. In practice, these are widely used, and are believed unbreakable in

                practice by most competent observers. There are systems similar to RSA, such as one by Michael O. Rabin

                that are provably secure provided factoring n = pq is impossible; it is quite unusable in practice. The

                discrete logarithm problem is the basis for believing some other cryptosystems are secure, and again,

                there are related, less practical systems that are provably secure relative to the solvability or

                insolvability discrete log problem.[32]

                As well as being aware of cryptographic history, cryptographic algorithm and system designers must also

                sensibly consider probable future developments while working on their designs. For instance, continuous

                improvements in computer processing power have increased the scope of brute-force attacks, so when

                specifying key lengths, the required key lengths are similarly advancing.[33] The potential effects of

                quantum computing are already being considered by some cryptographic system designers developing

                post-quantum cryptography; the announced imminence of small implementations of these machines may be

                making the need for preemptive caution rather more than merely speculative.

            </p>

            <!-- img of NSA involvement -->

            <img

                src="https://www.edureka.co/blog/wp-content/uploads/2018/07/sending-message-over-network-what-is-cryptography-edureka-1.png">

        </div>

1. NSA involvement

  <div id="NSA involvement">

            <p>

                Another contentious issue connected to cryptography in the United States is the influence of the

                National Security Agency on cipher development and policy.[8] The NSA was involved with the design of

                DES during its development at IBM and its consideration by the National Bureau of Standards as a

                possible Federal Standard for cryptography.[68] DES was designed to be resistant to differential

                cryptanalysis,[69] a powerful and general cryptanalytic technique known to the NSA and IBM, that became

                publicly known only when it was rediscovered in the late 1980s.[70] According to Steven Levy, IBM

                discovered differential cryptanalysis,[64] but kept the technique secret at the NSA's request. The

                technique became publicly known only when Biham and Shamir re-discovered and announced it some years

                later. The entire affair illustrates the difficulty of determining what resources and knowledge an

                attacker might actually have.

                Another instance of the NSA's involvement was the 1993 Clipper chip affair, an encryption microchip

                intended to be part of the Capstone cryptography-control initiative. Clipper was widely criticized by

                cryptographers for two reasons. The cipher algorithm (called Skipjack) was then classified (declassified

                in 1998, long after the Clipper initiative lapsed). The classified cipher caused concerns that the NSA

                had deliberately made the cipher weak in order to assist its intelligence efforts. The whole initiative

                was also criticized based on its violation of Kerckhoffs's Principle, as the scheme included a special

                escrow key held by the government for use by law enforcement (i.e. wiretapping).

            </p>

        </div>

1. Digital manegment

        <div id="digital manegment">

            Cryptography is central to digital rights management (DRM), a group of techniques for technologically

            controlling use of copyrighted material, being widely implemented and deployed at the behest of some

            copyright holders. In 1998, U.S. President Bill Clinton signed the Digital Millennium Copyright Act (DMCA),

            which criminalized all production, dissemination, and use of certain cryptanalytic techniques and technology

            (now known or later discovered); specifically, those that could be used to circumvent DRM technological

            schemes.[71] This had a noticeable impact on the cryptography research community since an argument can be

            made that any cryptanalytic research violated the DMCA. Similar statutes have since been enacted in several

            countries and regions, including the implementation in the EU Copyright Directive. Similar restrictions are

            called for by treaties signed by World Intellectual Property Organization member-states.

            The United States Department of Justice and FBI have not enforced the DMCA as rigorously as had been feared

            by some, but the law, nonetheless, remains a controversial one. Niels Ferguson, a well-respected

            cryptography researcher, has publicly stated that he will not release some of his research into an Intel

            security design for fear of prosecution under the DMCA.[72] Cryptologist Bruce Schneier has argued that the

            DMCA encourages vendor lock-in, while inhibiting actual measures toward cyber-security.[73] Both Alan Cox

            (longtime Linux kernel developer) and Edward Felten (and some of his students at Princeton) have encountered

            problems related to the Act. Dmitry Sklyarov was arrested during a visit to the US from Russia, and jailed

            for five months pending trial for alleged violations of the DMCA arising from work he had done in Russia,

            where the work was legal. In 2007, the cryptographic keys responsible for Blu-ray and HD DVD content

            scrambling were discovered and released onto the Internet. In both cases, the Motion Picture Association of

            America sent out numerous DMCA takedown notices, and there was a massive Internet backlash[9] triggered by

            the perceived impact of such notices on fair use and free speech.

            In the United Kingdom, the Regulation of Investigatory Powers Act gives UK police the powers to force

            suspects to decrypt files or hand over passwords that protect encryption keys. Failure to comply is an

            offense in its own right, punishable on conviction by a two-year jail sentence or up to five years in cases

            involving national security.[7] Successful prosecutions have occurred under the Act; the first, in 2009,[74]

            resulted in a term of 13 months' imprisonment.[75] Similar forced disclosure laws in Australia, Finland,

            France, and India compel individual suspects under investigation to hand over encryption keys or passwords

            during a criminal investigation.

            In the United States, the federal criminal case of United States v. Fricosu addressed whether a search

            warrant can compel a person to reveal an encryption passphrase or password.[76] The Electronic Frontier

            Foundation (EFF) argued that this is a violation of the protection from self-incrimination given by the

            Fifth Amendment.[77] In 2012, the court ruled that under the All Writs Act, the defendant was required to

            produce an unencrypted hard drive for the court.[78]

            In many jurisdictions, the legal status of forced disclosure remains unclear.

            The 2016 FBI–Apple encryption dispute concerns the ability of courts in the United States to compel

            manufacturers' assistance in unlocking cell phones whose contents are cryptographically protected.

            As a potential counter-measure to forced disclosure some cryptographic software supports plausible

            deniability, where the encrypted data is indistinguishable from unused random data (for example such as that

            of a drive which has been securely wiped).

        </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="#modren cryptography">modren cryptography</a></li>

            <li><a href="#NSA involvement">NSA involvement </a></li>

            <li><a href="#digital manegment">digital manegment </a></li>

        </ul>

    </header>

    <main>

        <div id="home">

            <p>

                The first use of the term cryptograph (as opposed to cryptogram) dates back to the 19th

                century—originating from The Gold-Bug, a story by Edgar Allan Poe.[10][11][broken footnote]

                Until modern times, cryptography referred almost exclusively to encryption, which is the process of

                converting ordinary information (called plaintext) into unintelligible form (called ciphertext).[12]

                Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.

                A cipher (or cypher) is a pair of algorithms that carry out the encryption and the reversing decryption.

                The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a

                "key". The key is a secret (ideally known only to the communicants), usually a string of characters

                (ideally short so it can be remembered by the user), which is needed to decrypt the ciphertext. In

                formal mathematical terms, a "cryptosystem" is the ordered list of elements of finite possible

                plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption

                algorithms which correspond to each key. Keys are important both formally and in actual practice, as

                ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are

                therefore useless (or even counter-productive) for most purposes.

                Historically, ciphers were often used directly for encryption or decryption without additional

                procedures such as authentication or integrity checks. There are, generally, two kinds of cryptosystems:

                symmetric and asymmetric. In symmetric systems, the only ones known until the 1970s, the same key (the

                secret key) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster

                than asymmetric systems in part because they generally use shorter key lengths. Asymmetric systems use a

                "public key" to encrypt a message and a related "private key" to decrypt it. The use of asymmetric

                systems enhances the security of communication, largely because the relation between the two keys is

                very hard to discover.[13] Examples of asymmetric systems include RSA (Rivest–Shamir–Adleman), and ECC

                (Elliptic Curve Cryptography). Quality symmetric algorithms include the commonly used AES (Advanced

                Encryption Standard) which replaced the older DES (Data Encryption Standard).[14] Not very high quality

                symmetric algorithms include the assorted children's language tangling schemes such as Pig Latin or

                other cant, and indeed effectively all cryptographic schemes, however seriously intended, from any

                source prior to the invention of the one-time pad early in the 20th century.

                In colloquial use, the term "code" is often used to mean any method of encryption or concealment of

                meaning. However, in cryptography, code has a more specific meaning: the replacement of a unit of

                plaintext (i.e., a meaningful word or phrase) with a code word (for example, "wallaby" replaces "attack

                at dawn"). A cypher, in contrast, is a scheme for changing or substituting an element below such a level

                (a letter, or a syllable or a pair of letters or ...) in order to produce a cyphertext.

                Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted

                information without access to the key normally required to do so; i.e., it is the study of how to

                "crack" encryption algorithms or their implementations.

                Some use the terms cryptography and cryptology interchangeably in English, while others (including US

                military practice generally) use cryptography to refer specifically to the use and practice of

                cryptographic techniques and cryptology to refer to the combined study of cryptography and

                cryptanalysis.[15][16] English is more flexible than several other languages in which cryptology (done

                by cryptologists) is always used in the second sense above. RFC 2828 advises that steganography is

                sometimes included in cryptology.[17]

                The study of characteristics of languages that have some application in cryptography or cryptology (e.g.

                frequency data, letter combinations, universal patterns, etc.) is called cryptolinguistics.

            </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="modren cryptography">

            <p>

                Cryptanalysis of the new mechanical devices proved to be both difficult and laborious. In the United

                Kingdom, cryptanalytic efforts at Bletchley Park during WWII spurred the development of more efficient

                means for carrying out repetitious tasks. This culminated in the development of the Colossus, the

                world's first fully electronic, digital, programmable computer, which assisted in the decryption of

                ciphers generated by the German Army's Lorenz SZ40/42 machine.

                Extensive open academic research into cryptography is relatively recent; it began only in the mid-1970s.

                In recent times, IBM personnel designed the algorithm that became the Federal (i.e., US) Data Encryption

                Standard; Whitfield Diffie and Martin Hellman published their key agreement algorithm;[31] and the RSA

                algorithm was published in Martin Gardner's Scientific American column. Since then, cryptography has

                become a widely used tool in communications, computer networks, and computer security generally.

                Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems

                are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep

                connections with abstract mathematics. There are very few cryptosystems that are proven to be

                unconditionally secure. The one-time pad is one, and was proven to be so by Claude Shannon. There are a

                few important algorithms that have been proven secure under certain assumptions. For example, the

                infeasibility of factoring extremely large integers is the basis for believing that RSA is secure, and

                some other systems, but even so, proof of unbreakability is unavailable since the underlying

                mathematical problem remains open. In practice, these are widely used, and are believed unbreakable in

                practice by most competent observers. There are systems similar to RSA, such as one by Michael O. Rabin

                that are provably secure provided factoring n = pq is impossible; it is quite unusable in practice. The

                discrete logarithm problem is the basis for believing some other cryptosystems are secure, and again,

                there are related, less practical systems that are provably secure relative to the solvability or

                insolvability discrete log problem.[32]

                As well as being aware of cryptographic history, cryptographic algorithm and system designers must also

                sensibly consider probable future developments while working on their designs. For instance, continuous

                improvements in computer processing power have increased the scope of brute-force attacks, so when

                specifying key lengths, the required key lengths are similarly advancing.[33] The potential effects of

                quantum computing are already being considered by some cryptographic system designers developing

                post-quantum cryptography; the announced imminence of small implementations of these machines may be

                making the need for preemptive caution rather more than merely speculative.

            </p>

            <!-- img of NSA involvement -->

            <img

                src="https://www.edureka.co/blog/wp-content/uploads/2018/07/sending-message-over-network-what-is-cryptography-edureka-1.png">

        </div>

        <div id="NSA involvement">

            <p>

                Another contentious issue connected to cryptography in the United States is the influence of the

                National Security Agency on cipher development and policy.[8] The NSA was involved with the design of

                DES during its development at IBM and its consideration by the National Bureau of Standards as a

                possible Federal Standard for cryptography.[68] DES was designed to be resistant to differential

                cryptanalysis,[69] a powerful and general cryptanalytic technique known to the NSA and IBM, that became

                publicly known only when it was rediscovered in the late 1980s.[70] According to Steven Levy, IBM

                discovered differential cryptanalysis,[64] but kept the technique secret at the NSA's request. The

                technique became publicly known only when Biham and Shamir re-discovered and announced it some years

                later. The entire affair illustrates the difficulty of determining what resources and knowledge an

                attacker might actually have.

                Another instance of the NSA's involvement was the 1993 Clipper chip affair, an encryption microchip

                intended to be part of the Capstone cryptography-control initiative. Clipper was widely criticized by

                cryptographers for two reasons. The cipher algorithm (called Skipjack) was then classified (declassified

                in 1998, long after the Clipper initiative lapsed). The classified cipher caused concerns that the NSA

                had deliberately made the cipher weak in order to assist its intelligence efforts. The whole initiative

                was also criticized based on its violation of Kerckhoffs's Principle, as the scheme included a special

                escrow key held by the government for use by law enforcement (i.e. wiretapping).

            </p>

        </div>

        <div id="digital manegment">

            Cryptography is central to digital rights management (DRM), a group of techniques for technologically

            controlling use of copyrighted material, being widely implemented and deployed at the behest of some

            copyright holders. In 1998, U.S. President Bill Clinton signed the Digital Millennium Copyright Act (DMCA),

            which criminalized all production, dissemination, and use of certain cryptanalytic techniques and technology

            (now known or later discovered); specifically, those that could be used to circumvent DRM technological

            schemes.[71] This had a noticeable impact on the cryptography research community since an argument can be

            made that any cryptanalytic research violated the DMCA. Similar statutes have since been enacted in several

            countries and regions, including the implementation in the EU Copyright Directive. Similar restrictions are

            called for by treaties signed by World Intellectual Property Organization member-states.

            The United States Department of Justice and FBI have not enforced the DMCA as rigorously as had been feared

            by some, but the law, nonetheless, remains a controversial one. Niels Ferguson, a well-respected

            cryptography researcher, has publicly stated that he will not release some of his research into an Intel

            security design for fear of prosecution under the DMCA.[72] Cryptologist Bruce Schneier has argued that the

            DMCA encourages vendor lock-in, while inhibiting actual measures toward cyber-security.[73] Both Alan Cox

            (longtime Linux kernel developer) and Edward Felten (and some of his students at Princeton) have encountered

            problems related to the Act. Dmitry Sklyarov was arrested during a visit to the US from Russia, and jailed

            for five months pending trial for alleged violations of the DMCA arising from work he had done in Russia,

            where the work was legal. In 2007, the cryptographic keys responsible for Blu-ray and HD DVD content

            scrambling were discovered and released onto the Internet. In both cases, the Motion Picture Association of

            America sent out numerous DMCA takedown notices, and there was a massive Internet backlash[9] triggered by

            the perceived impact of such notices on fair use and free speech.

            In the United Kingdom, the Regulation of Investigatory Powers Act gives UK police the powers to force

            suspects to decrypt files or hand over passwords that protect encryption keys. Failure to comply is an

            offense in its own right, punishable on conviction by a two-year jail sentence or up to five years in cases

            involving national security.[7] Successful prosecutions have occurred under the Act; the first, in 2009,[74]

            resulted in a term of 13 months' imprisonment.[75] Similar forced disclosure laws in Australia, Finland,

            France, and India compel individual suspects under investigation to hand over encryption keys or passwords

            during a criminal investigation.

            In the United States, the federal criminal case of United States v. Fricosu addressed whether a search

            warrant can compel a person to reveal an encryption passphrase or password.[76] The Electronic Frontier

            Foundation (EFF) argued that this is a violation of the protection from self-incrimination given by the

            Fifth Amendment.[77] In 2012, the court ruled that under the All Writs Act, the defendant was required to

            produce an unencrypted hard drive for the court.[78]

            In many jurisdictions, the legal status of forced disclosure remains unclear.

            The 2016 FBI–Apple encryption dispute concerns the ability of courts in the United States to compel

            manufacturers' assistance in unlocking cell phones whose contents are cryptographically protected.

            As a potential counter-measure to forced disclosure some cryptographic software supports plausible

            deniability, where the encrypted data is indistinguishable from unused random data (for example such as that

            of a drive which has been securely wiped).

        </div>

    </main>

</body>

</html>