Name : حسن ابراهيم محمد سالم

ID : 286

Group: 3

Sec:13

GitHub page:

GitHub Link :

* Cryptography system 5 webpage
* 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>

* 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>

* Symetric-key

<div id="Symmetric-key">

<p>

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the

same key (or, less commonly, in which their keys are different, but related in an easily computable

way). This was the only kind of encryption publicly known until June 1976.[31]

logic diagram showing International Data Encryption Algorithm cypher process

One round (out of 8.5) of the IDEA cipher, used in most versions of PGP and OpenPGP compatible software

for time-efficient encryption of messages

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher

enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a

stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs

that have been designated cryptography standards by the US government (though DES's designation was

finally withdrawn after the AES was adopted).[34] Despite its deprecation as an official standard, DES

(especially its still-approved and much more secure triple-DES variant) remains quite popular; it is

used across a wide range of applications, from ATM encryption[35] to e-mail privacy[36] and secure

remote access.[37] Many other block ciphers have been designed and released, with considerable variation

in quality. Many, even some designed by capable practitioners, have been thoroughly broken, such as

FEAL.[4][38]

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material,

which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time

pad. In a stream cipher, the output stream is created based on a hidden internal state that changes as

the cipher operates. That internal state is initially set up using the secret key material. RC4 is a

widely used stream cipher.[4] Block ciphers can be used as stream ciphers by generating blocks of a

keystream (in place of a Pseudorandom number generator) and applying an XOR operation to each bit of the

plaintext with each bit of the keystream.[39]

Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any

length as input, and output a short, fixed-length hash, which can be used in (for example) a digital

signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4

is a long-used hash function that is now broken; MD5, a strengthened variant of MD4, is also widely used

but broken in practice. The US National Security Agency developed the Secure Hash Algorithm series of

MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed

and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family

improves on SHA-1, but is vulnerable to clashes as of 2011; and the US standards authority thought it

"prudent" from a security perspective to develop a new standard to "significantly improve the robustness

of NIST's overall hash algorithm toolkit."[40] Thus, a hash function design competition was meant to

select a new U.S. national standard, to be called SHA-3, by 2012. The competition ended on October 2,

2012, when the NIST announced that Keccak would be the new SHA-3 hash algorithm.[41] Unlike block and

stream ciphers that are invertible, cryptographic hash functions produce a hashed output that cannot be

used to retrieve the original input data. Cryptographic hash functions are used to verify the

authenticity of data retrieved from an untrusted source or to add a layer of security.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key

can be used to authenticate the hash value upon receipt;[4] this additional complication blocks an

attack scheme against bare digest algorithms, and so has been thought worth the effort.

</p>

</div>

* Public--key

<div id="Public-key ">

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, although a message

or group of messages can have a different key than others. A significant disadvantage of symmetric ciphers

is the key management necessary to use them securely. Each distinct pair of communicating parties must,

ideally, share a different key, and perhaps for each ciphertext exchanged as well. The number of keys

required increases as the square of the number of network members, which very quickly requires complex key

management schemes to keep them all consistent and secret.

<!-- img of NSA involvement -->

<img

src="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTorAoce5qVTLrYCqKnjqZ4i-oE2yTMvlrDig&usqp=CAU">

</div>

* cryptosystems

<div id="Cryptosystems">

<p>

One or more cryptographic primitives are often used to develop a more complex algorithm, called a

cryptographic system, or cryptosystem. Cryptosystems (e.g., El-Gamal encryption) are designed to provide

particular functionality (e.g., public key encryption) while guaranteeing certain security properties

(e.g., chosen-plaintext attack (CPA) security in the random oracle model). Cryptosystems use the

properties of the underlying cryptographic primitives to support the system's security properties. As

the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem

can be derived from a combination of several more primitive cryptosystems. In many cases, the

cryptosystem's structure involves back and forth communication among two or more parties in space (e.g.,

between the sender of a secure message and its receiver) or across time (e.g., cryptographically

protected backup data). Such cryptosystems are sometimes called cryptographic protocols.

Some widely known cryptosystems include RSA encryption, Schnorr signature, El-Gamal encryption, PGP,

etc. More complex cryptosystems include electronic cash[54] systems, signcryption systems, etc. Some

more 'theoretical'[clarification needed] cryptosystems include interactive proof systems,[55] (like

zero-knowledge proofs),[56] systems for secret sharing.

</p>

</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="#Symmetric-key">Symmetric-key</a></li>

<li><a href="#Public-key ">Public-key </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="Symmetric-key">

<p>

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the

same key (or, less commonly, in which their keys are different, but related in an easily computable

way). This was the only kind of encryption publicly known until June 1976.[31]

logic diagram showing International Data Encryption Algorithm cypher process

One round (out of 8.5) of the IDEA cipher, used in most versions of PGP and OpenPGP compatible software

for time-efficient encryption of messages

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher

enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a

stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs

that have been designated cryptography standards by the US government (though DES's designation was

finally withdrawn after the AES was adopted).[34] Despite its deprecation as an official standard, DES

(especially its still-approved and much more secure triple-DES variant) remains quite popular; it is

used across a wide range of applications, from ATM encryption[35] to e-mail privacy[36] and secure

remote access.[37] Many other block ciphers have been designed and released, with considerable variation

in quality. Many, even some designed by capable practitioners, have been thoroughly broken, such as

FEAL.[4][38]

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material,

which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time

pad. In a stream cipher, the output stream is created based on a hidden internal state that changes as

the cipher operates. That internal state is initially set up using the secret key material. RC4 is a

widely used stream cipher.[4] Block ciphers can be used as stream ciphers by generating blocks of a

keystream (in place of a Pseudorandom number generator) and applying an XOR operation to each bit of the

plaintext with each bit of the keystream.[39]

Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any

length as input, and output a short, fixed-length hash, which can be used in (for example) a digital

signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4

is a long-used hash function that is now broken; MD5, a strengthened variant of MD4, is also widely used

but broken in practice. The US National Security Agency developed the Secure Hash Algorithm series of

MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed

and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family

improves on SHA-1, but is vulnerable to clashes as of 2011; and the US standards authority thought it

"prudent" from a security perspective to develop a new standard to "significantly improve the robustness

of NIST's overall hash algorithm toolkit."[40] Thus, a hash function design competition was meant to

select a new U.S. national standard, to be called SHA-3, by 2012. The competition ended on October 2,

2012, when the NIST announced that Keccak would be the new SHA-3 hash algorithm.[41] Unlike block and

stream ciphers that are invertible, cryptographic hash functions produce a hashed output that cannot be

used to retrieve the original input data. Cryptographic hash functions are used to verify the

authenticity of data retrieved from an untrusted source or to add a layer of security.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key

can be used to authenticate the hash value upon receipt;[4] this additional complication blocks an

attack scheme against bare digest algorithms, and so has been thought worth the effort.

</p>

</div>

<div id="Public-key ">

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, although a message

or group of messages can have a different key than others. A significant disadvantage of symmetric ciphers

is the key management necessary to use them securely. Each distinct pair of communicating parties must,

ideally, share a different key, and perhaps for each ciphertext exchanged as well. The number of keys

required increases as the square of the number of network members, which very quickly requires complex key

management schemes to keep them all consistent and secret.

<!-- img of NSA involvement -->

<img

src="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTorAoce5qVTLrYCqKnjqZ4i-oE2yTMvlrDig&usqp=CAU">

</div>

<div id="Cryptosystems">

<p>

One or more cryptographic primitives are often used to develop a more complex algorithm, called a

cryptographic system, or cryptosystem. Cryptosystems (e.g., El-Gamal encryption) are designed to provide

particular functionality (e.g., public key encryption) while guaranteeing certain security properties

(e.g., chosen-plaintext attack (CPA) security in the random oracle model). Cryptosystems use the

properties of the underlying cryptographic primitives to support the system's security properties. As

the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem

can be derived from a combination of several more primitive cryptosystems. In many cases, the

cryptosystem's structure involves back and forth communication among two or more parties in space (e.g.,

between the sender of a secure message and its receiver) or across time (e.g., cryptographically

protected backup data). Such cryptosystems are sometimes called cryptographic protocols.

Some widely known cryptosystems include RSA encryption, Schnorr signature, El-Gamal encryption, PGP,

etc. More complex cryptosystems include electronic cash[54] systems, signcryption systems, etc. Some

more 'theoretical'[clarification needed] cryptosystems include interactive proof systems,[55] (like

zero-knowledge proofs),[56] systems for secret sharing.

</p>

</div>

</main>

</body>

</html>