RSA

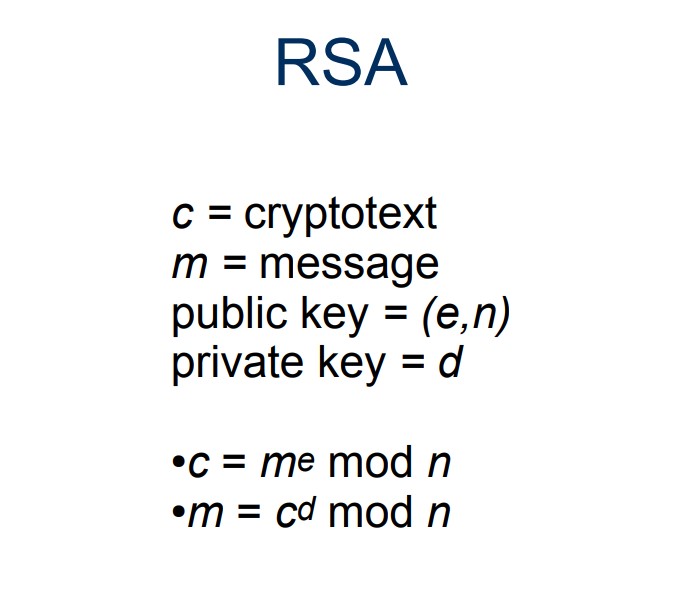
Good key size – 1024

2K generally today

3072

Prime numbers easy to find

Factors of large numbers hard to find



RSA can’t be used to encrypt large texts as it will result in very large ciphertext.

CBC stands for Cipher Block Chaining, a mode of operation used with block ciphers in cryptography. It's a method to encrypt data in blocks, which enhances the security of the encryption process compared to encrypting each block individually.

1. **Block Cipher**: In block cipher encryption, the plaintext (data to be encrypted) is divided into fixed-size blocks, and each block is encrypted separately.
2. **Initial Vector (IV)**: CBC mode requires an initial vector (IV) for the first block of data. The IV is a random string of bits that is as long as the block size. It should be unpredictable and unique for each encryption session to ensure security.
3. **Chaining Mechanism**: In CBC mode, each block of plaintext is XOR-ed (exclusive OR operation) with the previous block's ciphertext before being encrypted. This means the ciphertext of one block depends on the plaintext and the ciphertext of all previous blocks.

Which of the following are true statements about block and stream ciphers?

1.

Block ciphers suffer from error propagation, where an error affects the transformation of all other characters in the same block.

2.

Stream ciphers commonly run in CBC mode

3.

DES can be used as basis for a stream cipher.

4.

Stream ciphers are generally faster than block ciphers for encrypting large amounts of data.

Feedback

Your answer is correct.

The correct answers are:

Block ciphers suffer from error propagation, where an error affects the transformation of all other characters in the same block.,

Stream ciphers are generally faster than block ciphers for encrypting large amounts of data.

DES is fundamentally for a block cipher.

The RSA algorithm is now assumed to have a limited future because

Select one or more:

a)

five qubits are enough to break RSA encryption

b)

quantum computers have been shown to be able to factor integers in ways that normal computers cannot

c)

quantum computing promises new encryption methods that are guaranteed to be safe.

d)

quantum computers are much faster than conventional computers for all computations.

Feedback

Your answer is incorrect.

The correct answers are: quantum computers have been shown to be able to factor integers in ways that normal computers cannot, quantum computing promises new encryption methods that are guaranteed to be safe.

A qubit, short for "quantum bit," is the fundamental unit of quantum information in quantum computing. It represents a new way of processing data, fundamentally different from the traditional bits used in classical computing.

Here's a breakdown of what qubits are and how they work:

1. **Classical Bits vs. Qubits**:
   * In classical computing, a bit is the basic unit of information and can exist in one of two states: 0 or 1.
   * A qubit, on the other hand, can exist not only in the traditional binary states of 0 or 1 but also in a superposition of both states simultaneously, thanks to the principles of quantum mechanics.
2. **Superposition**:
   * Superposition is a quantum mechanical phenomenon where a quantum system can be in multiple states at the same time. For a qubit, this means it can be 0, 1, or any quantum superposition of these states.
3. **Entanglement**:
   * Another key property of qubits is entanglement, which is a strong correlation that exists between quantum particles. When qubits become entangled, the state of one qubit is directly related to the state of another, no matter the distance between them. This property is crucial for quantum computing and communication.
4. **Quantum Computing**:
   * In quantum computing, qubits are manipulated using quantum gates and algorithms. Due to superposition and entanglement, quantum computers can process a vast amount of data and solve certain problems much faster than classical computers.
5. **Challenges**:
   * Qubits are extremely sensitive to their environment, a phenomenon known as quantum decoherence. Maintaining the stability of qubits (i.e., keeping them in a coherent quantum state) for a sufficient duration to perform computations is a significant challenge in quantum computing.
6. **Potential Applications**:
   * Quantum computing, powered by qubits, holds the potential to revolutionize various fields, including cryptography, drug discovery, optimization problems, and more, by solving complex problems that are currently intractable for classical computers.

In summary, qubits are the basic units of quantum information that exploit quantum mechanical properties like superposition and entanglement, offering a new paradigm in computing with the potential for immense computational power. However, practical and widespread use of quantum computing is still in the developmental stages, facing various technical challenges.

Quantum key distribution(QKD) is a secure communication method that implements a protocol involving components of quantum mechanics.

When you get to quantum level can’t observe things without changing.

If you get a polarizing filter that filters out those and one that filters out those ,it’s not black anymore.

Quantum systems vulnerable to denial of service attacks.

The correct answer is:

BitCoin is the best known example of a [crytpocurrency].  There is no central authority that controls the currency, that is to say it is entirely [peer to peer]. Lists of payments are links together in a so called [block chain] that contains the entire history of all the BitCoin transactions from the beginning. This data structure is copied, spread and maintained around the world in what is called a [distributed ledger] - a basic principle that promises many more revolutionary applications in the future besides its use in BitCoin.

True. Blockchain is indeed commonly described as a decentralized, immutable ledger. Here's a brief explanation of these characteristics:

1. **Decentralized**: Blockchain technology operates on a distributed network of computers. Instead of having a central authority or server, the blockchain is maintained by multiple nodes (computers) that participate in the network. Each node has a copy of the entire ledger, making the system decentralized.
2. **Immutable Ledger**: Once a transaction is recorded on the blockchain, it cannot be altered or deleted. This immutability is ensured through cryptographic hashing and the consensus mechanism used by the network. When a block of transactions is added to the blockchain, altering its content would require not only recalculating the hash of the altered block but also the hashes of all subsequent blocks, which is computationally impractical, especially given the decentralized nature of the network where each node maintains a copy of the ledger.

This combination of decentralization and immutability makes blockchain a robust and transparent system for recording transactions, and it's the foundation of technologies like cryptocurrencies, smart contracts, and various other applications that require a secure, transparent, and tamper-proof record-keeping mechanism.

Can crack a vigenere cipher in few days using Kasiski method.

Cryptography is hiding things.

Hashes is representing things in a short way.

HMAC

HMAC is a algorithm that uses a keyless hash function .

HMAC stands for Hash-based Message Authentication Code. It is a type of cryptographic function used to verify both the integrity and the authenticity of a message. HMAC combines a cryptographic hash function with a secret cryptographic key and is widely used in various security applications and protocols.

Here's a more detailed explanation of HMAC:

1. **Cryptographic Hash Function**: A hash function takes an input (or 'message') and returns a fixed-size string of bytes. The output is typically a 'digest' that is unique to each unique input. Common hash functions include SHA-256, MD5, and SHA-1.
2. **Combining with a Secret Key**: In HMAC, the hash function is combined with a secret key. This key is known only to the sender and intended receiver, adding a layer of security. The process generally involves hashing the key and message in a specific way to produce the HMAC value.
3. **Process**:

The original message is combined with a secret key.

The combined message and key are then passed through the hash function.

The resulting hash (the HMAC) is appended to the message or sent alongside it.

1. **Verification**: Upon receiving the message and the HMAC, the receiver:
   * Combines the received message with the same secret key and applies the same hash function.
   * Compares the resulting HMAC with the received HMAC.
   * If they match, it confirms that the message has not been altered and is authentic, as only someone with the correct key could have created the matching HMAC.
2. **Uses**:
   * HMAC is used in various security applications where data integrity and authentication are crucial.
   * It is commonly used in digital signatures, message integrity checks, and in various network communication protocols.
3. **Advantages**:
   * The combination of a hash function with a secret key in HMAC makes it more secure against certain attacks compared to using a hash function alone.
   * HMAC provides assurance about both the data integrity (the data hasn't been tampered with) and authenticity (the data comes from a legitimate source).

In summary, HMAC is a secure method for verifying both the integrity and the authenticity of digital messages, providing an additional layer of security in cryptographic communications.

10 boxes and 11 things to put in ,one has to have 2 things in it.

Complete work of Shakespeare-64 bit

Bible-64 bit

We hashed 2^64 documents ,we used all bits hash of 2 things will be same.

Make it bigger and bigger ,so very less chance 2 things have the same hash.

The correct answer is: A symmetrical  encryption algorithm and substitutional cipher that can in principle be unbreakable → One time pad, An asymmetrical algorithm invented in the 1970s → RSA, A symmetrical algorithm with key length of 64 bits → DES, A symmetrical algorithm with keyspace up to 2256 → AES

No need to study elliptic curve ciphers in detail.

No need How they will work.

Just another way to implement public key cryptography.

Hashes is about integrity.

Yes, in the context of computer security and cryptography, a hash is indeed used to ensure the integrity of data. Hash functions are designed to take an input (or 'message') and return a fixed-size string of characters, which is typically a digital fingerprint of the input.

Here's how hashing relates to integrity:

1. **Fixed-Size Output**: Regardless of the size of the input data, a hash function produces a fixed-size output (often called a hash code or digest). Common hash functions include SHA-256, SHA-1, and MD5, each producing outputs of a specific length.
2. **Uniqueness**: A good hash function has the property that it is computationally infeasible to find two different inputs that produce the same output hash. This uniqueness is critical for ensuring data integrity.
3. **Sensitivity to Changes**: Hash functions are highly sensitive to changes in the input data. Even a small change in the input (like modifying a single character) will produce a significantly different output hash. This property is known as the avalanche effect.
4. **Verifying Integrity**: Hashes are commonly used to verify data integrity. When data is transmitted or stored, its hash can be calculated and sent or stored along with it. The recipient or a future user can recompute the hash on the received or retrieved data and compare it to the original hash. If the hashes match, it ensures that the data has not been altered; if they don't, it indicates that the data may have been compromised or corrupted.
5. **Non-reversibility**: Hash functions are one-way functions; it is computationally infeasible to reverse the process, i.e., to derive the original input data from its hash. This property is important for security purposes but also underscores the fact that hashing, by itself, does not encrypt or hide the original data.
6. **Usage in Security**: Beyond ensuring data integrity, hashes are used in various other security applications, such as in the formation of digital signatures and in the process of user authentication (storing hashed passwords).

In summary, hashes play a crucial role in maintaining the integrity of data in various computing and security contexts. They provide a way to detect any alterations in data, which is fundamental to trust and reliability in digital communications and data storage.

Replay attack