Data Encryption & Cryptography Glossary

http://glossary-of-terms.ru/?do=g&v=39

Английский	
backup tapes Copying data on tapes for the purpose of restoring the original content in case data is lost.	
block cipher A block cipher a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length.	
california sb 1386 California senate bill requires that organizations that own or have access to personal information of california residents to notify them if the security of their information is compromised.	
ciphertext Unreadible text resulting from encryption.	шифртекст (полученный в результате шифрования текст) ~ associated with a givekey шифртекст, полученный на данном ключе
cryptography The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text.	криптография (наука о принципах, средствах и методах преобразования информации для защиты её от несанкционированного доступа и искажения) ~ textbook учебник [пособие / руководство] по криптографии
data encryption The process of converting data - known as plaintext - using an algorithm to make it unreadable.	
data storage Memory, components, media, and devices that retain digital and computer data for.	
data storage devices A device used for saving data. data is copied it recorded on to the device.	
decipher To convert from a code or cipher to plain text; decode.	
decrypt To convert from a code or cipher to plain text; decode.	
decryption Converting data from the unintelligible ciphertext back to plaintext. the reverse of data encryption.	
electronic data storage A storage device which requires electrical power to store and retrieve saved data.	
encipher 1. To convert plain text into an unintelligible form by means of a cipher. 2. Кодировать	кодировать шифровать
encrypt To convert plain text into an unintelligible form.	
encryption 1. The process of transforming text into an unintelligible form called cipher. 2. A method of encoding data for security. 3. Защита сообщения от неправомочного прочтения, основанная на преобразовании его в шифрованный текст. расшифровать этот текст, т.е. восстановить исходное сообщение, можно только с	шифрование ~ algorithm алгоритм шифрования

помощью ключа, использовавшегося при его шифровании 4. The rearrangement of the bit stream of a previously digitally encoded signal in a 5. An encoder electronically alters a signal so that it can be clearly seen only by recipients who have a decoder to reverse encryption. selective addressability/scrambling designates receivers to descramble a signal. each decoder has a unique address. 6. The rearrangement of the bit stream of a previously digitally encoded signal in a systematic fashion to make the information unrecognizable until restored on receipt of the necessary authorization key. this technique is used for securing information transmitted over a communication channel with the intent of excluding all other than authorized receivers from interpreting the message. can be used for voice, video and other communications signals. 7. Encryption is a process by which a document (plaintext) is combined with a shorter string of data, called a key (eg.), to produce an output (ciphertext) which can be "decrypted" back into the original plaintext by someone else who has the key, but which is incomprehensible and computationally infeasible to decrypt for anyone who does not have the key.	
encryption hardware Hardware device used to encrypt data. they are designed to work across a full range of operating systems and appear transparent to the operating system.	
encryption software Software used to encrypt and decrypt data, usually in the form of computer files, removable media, email messages, or in the form of packets sent over computer networks.	
gramm-leach-bliley act This act includes laws that govern the collection and disclosure of customers' personal financial information by financial institutions. it requires all financial institutions to design, implement and maintain safeguards to protect customer information.	
hipaa The health insurance portability and accountability act (hipaa) is a set of standards for the privacy and protection of all electronic health information. it includes a privacy rule and a security rule that requires healthcare organizations to increase th	
pci data security standard Payment card industry data security standard is a set of comprehensive requirements for enhancing payment account data security	
plain text Unencrypted text	
private key 1. A private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. 2. A private key is a string of data that shows you have access to bitcoins in a specific wallet. private keys can be thought of as a password; private keys must never be revealed to anyone but you, as they allow you to spend the bitcoins from your bitcoin wallet through a cryptographic signature.	частный ключ
public key A public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages.	общедоступный ключ
public key encryption 1. A form of encryption that utilizes a unique pair of keys, one (the "public key ") being openly known, and the other (the "private key "), being known only to the recipient of an encrypted message. 2. A special kind of encryption where there is a process for generating two keys at the same time (typically called a private key and a public key), such that documents encrypted using one key can be decrypted with the other. generally, as suggested by the name, individuals publish their public keys and keep their private keys to themselves.	
secure key management Trusted users are issued a key which enables them to access	

encrypted data.

storage encryption
Backup data stored is encrypted in an effort to prevent data theft and secure the kept data.

storage encryption appliance
Appliance used to encrypt data.

stream cipher
A stream cipher is a type of symmetric encryption algorithm. while block ciphers operate on large blocks of data, stream ciphers typically operate on smaller units of plaintext, usually bits.

triple des
Also referred to as 3des, a mode of the des encryption algorithm that encrypts data three times. three 64-bit keys are used, instead of one, for an overall key length of 192 bits.