A case study of abc institute of research

Business

Research has sensitive information that needs to be protected from TTS rivals.

The Institute has collaborated with EX. Inc. To research genetics. The information must be kept top secret at any cost. At BBC Institute, the researchers are unsure about the type of key (asymmetric or symmetric) to use. Please formulate a possible solution, and describe the advantages and disadvantages of any solution employed.

The best type of key to use in this situation would be public-key cryptography, also now as asymmetric cryptography.

It is a type of cryptographic algorithm that requires two separate keys. One of those keys is private, and kept secret. The other is public and distributed to those who need it. The keys are both needed since they are part of a mathematical algorithm, and one will not work without the other. This can be important in two ways.

First it can be used to encrypt plain text information like files and emails. Second, it can be used to verify the identity of the person you are communicating with. BBC institute will want to email back and forth with EX. Inc.

They can manage this Ninth using asymmetric keys. The sender will simply type the desired message and then use the public key of the person they wish to send the message for encrypting and therefore securing the message to be sent over the very public internet.

Having done this the only person who could possibly open and read this email would be the desired recipient. This is insured because since their public key was used to encrypt, the only way to decrypt the message into a readable email is by using the recipient’s private key which only they have access to.

At the same time the asymmetric system can be used to verify the parties involved. If I am sending a message to you, and you want to be sure that it is me and not an attacker trying to cause harm, all I need to do is sign the message with my private key. Since I am the only person in the world that has my private key, when {o use my public key to verify the message it will be decrypted.

Anyone else’s key Nil result in unreadable gibberish. This also becomes useful for online digital signatures of important documents. All of this is overseen by a certification authority.

If at any time a private key is lost or compromised in some way, that key is placed on a revocation list and will forever be out of use. That person will then be issued another secure key. Another way to further secure this system is by using smart cards to store the keys.

Each employee Nil be issued a smart card and they will be required to create a password to use them. Now they have a private key that only exists on their smart card that only they know the password two. This is multiracial security and by far the best way to go for this situation.