Asymmetric encryption

Business

So we use encryption to encode the ATA so that It requires a special key to be read that way you can protect your data. There are two types of encryption which are symmetric and asymmetric. So there Is two possible solutions to the dilemma we are facing, whether to use symmetric or asymmetric encryption to protect your research. With symmetric encryption, you run a file through the program and create a key that scrambles the file. Then you e-mail the encrypted file to the recipient and separately transmit the decoding key.

Running the same encryption application, the recipient uses the decoding key to unscramble the message. The only disadvantage of symmetric encryption is that while it’s fast it’s not as safe as asymmetric encryption because someone could intercept the key and decode the messages (Brandt, 2000). Asymmetric encryption is more complex but in turn is more secure than symmetric encryption. Two related keys are required when using asymmetric encryption. One key is a public key which is available to anyone who might send you any kind of encrypted Information.

That key can only encode data, It cannot decode It.

The second key Is a private key. Your private key stays safe with you, and when people wish to send you encrypted Information, they encrypt It sing your public key. When you receive the cipher text, you decrypt it with your private key. Asymmetric encryption’s added safety comes at a price though. It requires more computation.

So the process takes longer because it requires far more processing power to both encrypt and decrypt the content of the message. My recommendation for your venture would be to use Asymmetric encryption.

Even though the process may tang longer it’s more complex and harder to decode. It’s more secure than using symmetric encryption even though symmetric is faster, it would be easier to decode since someone could intercept and decode the message. Users can send secret messages by encrypting a message with the recipient’s public key. In this case, only the Intended recipient can decrypt the message, since only that user should have access to the required secret key.

In order to use asymmetric encryption, there Is a way that people use to discover other public keys.

The typical technique is that they use digital certificates. A certificate is a package of information Tanat elementals a user or a server, Ana contains International sun as ten organization name, the user’s e-mail address and country, the organization that issued the eradicate, and the user’s public key (Microsoft, 2012) In closing, Even though both symmetrical and asymmetrical encryption would work in your current situation, asymmetrical is far better because it’s more secure and harder to decode than symmetrical encryption even though it requires more processing power.