Pretty Good Privacy

is it actually pretty?

Muhammad Taimoor Hassan (P20-0603)
Armghan (P20-0183)

Try Pitch

What is PGP?

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

Try Pitch

How this "Pretty" thing works?

PGP is a program that uses public-key cryptography to provide secure communication. Public-key cryptography is a cryptographic system that uses pairs of keys.

- **Encryption**
- **Decryption**

Try Pitch

Encryption

When someone wants to send a message to another person using PGP,

1. First encrypt the message using the recipient's public key.
2. The sender can obtain the recipient's public key from a public key server or from the recipient directly.
3. Once the message is encrypted, only the recipient can decrypt it using their private key.

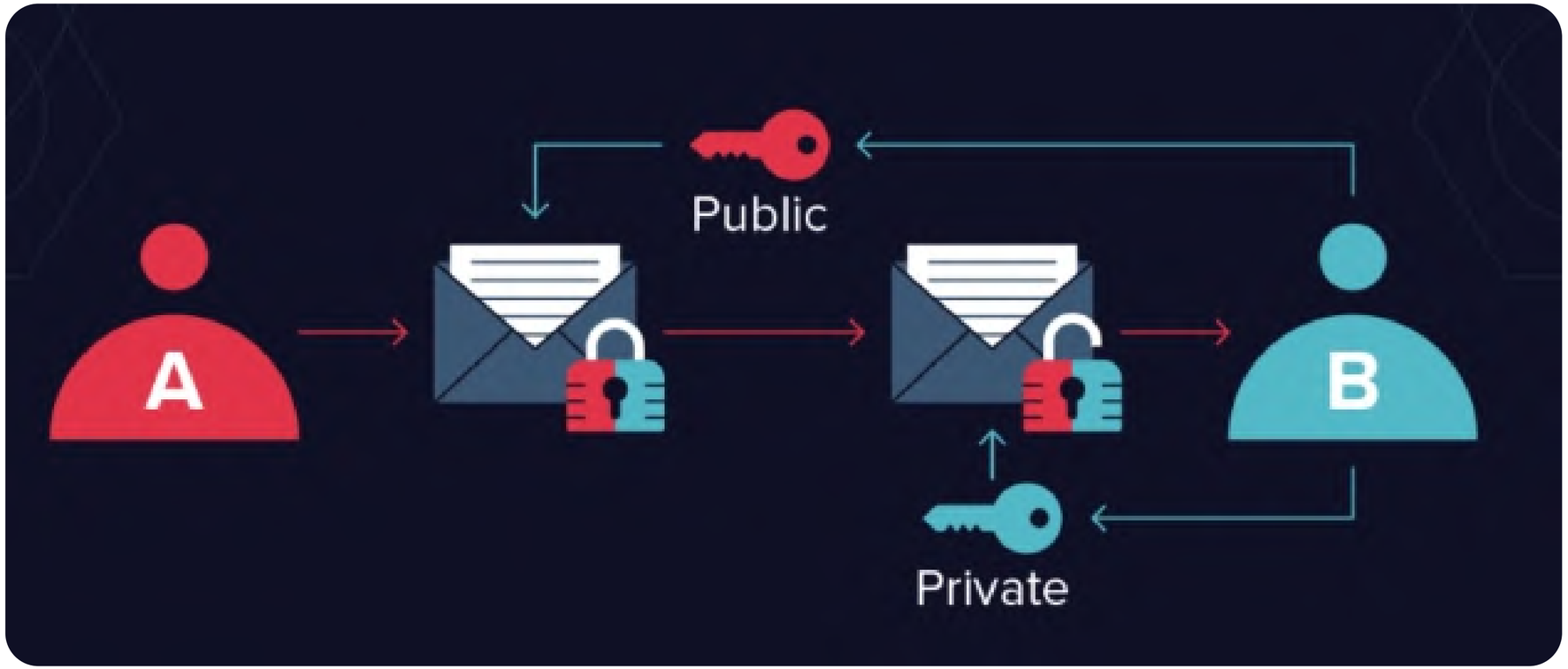
Try Pitch

Decryption

When the recipient receives the encrypted message,

1. They use their private key to decrypt it.
2. The decrypted message is then readable by the recipient. This process ensures that only the intended recipient can read the message, even if the message is intercepted during transmission.

Try Pitch



Try Pitch

Some "Pretty" Use Cases

- **Files Encryption**
  - Symmetric-key encryption to encrypt the contents. Same key is used to encrypt and decrypt the file. The key is generated from a passphrase provided by the user.
- **Verifying IDs or Digital Signatures**
  - Digital signatures are a way to verify the authenticity of a message or document.
- **Sending & Receiving Emails**
  - PGP generates a random symmetric key that is used to encrypt the message.

Try Pitch

Pros

- Extremely Secure
- Free to use
- End-to-End Encryption
- Key Management

Try Pitch

Cons

- Not User Friendly
- Requries Setup/Software
- No Anonymity
- Requires Proper Knowledge

Demo

Try Pitch

Thank you

Try Pitch