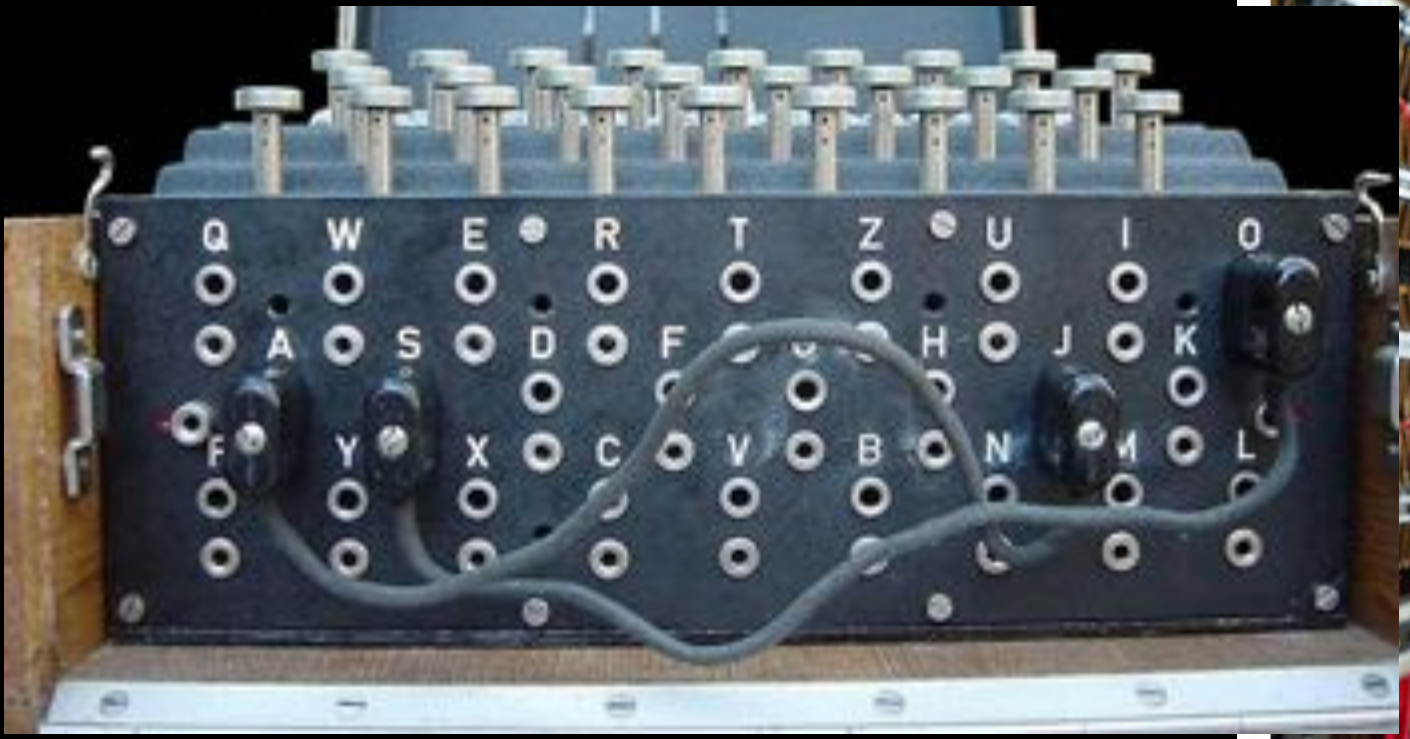
ENCRYPTION

Database Management System

Sujan Tamrakar

Reveal me:

PCOCUVG JGTG



The Imitation Game:

a movie about the Enigma Machine, Alan Turing and the Bletchley Park code-breakers

During World War II, the Germans used the Enigma machine to pass encrypted transmissions back and forth, which took years before the Polish were able to crack the messages, and give the solution to the Allied forces, which was instrumental to their victory.

- https://www.security.org/how-secure-is-my-password/
- https://www.youtube.com/watch?v=eWq5wAX8K8A
- https://www.youtube.com/watch?v=1y1M2fZqIlQ&t=320s

Encryption

- Plays a key role in protecting information & in authentication of users.
- Basic encryption technique may not provide adequate security, due to its simple computation.
- Ex: Cryptoarithmetic (substitution of character with next character or addition/subtraction)

[Rainbow table]

- Encryption consists of applying an encryption algorithm to data using some pre-specified encryption key. The resulting data has to be decrypted using a decryption key to recover the original data.
- Examples: MD5, AES, 3DES, Twofish, RSA, SALT, etc.


intel
Security
HOW PASSWORD
LENGTH WINS
THE INTERNET
Passwords 102

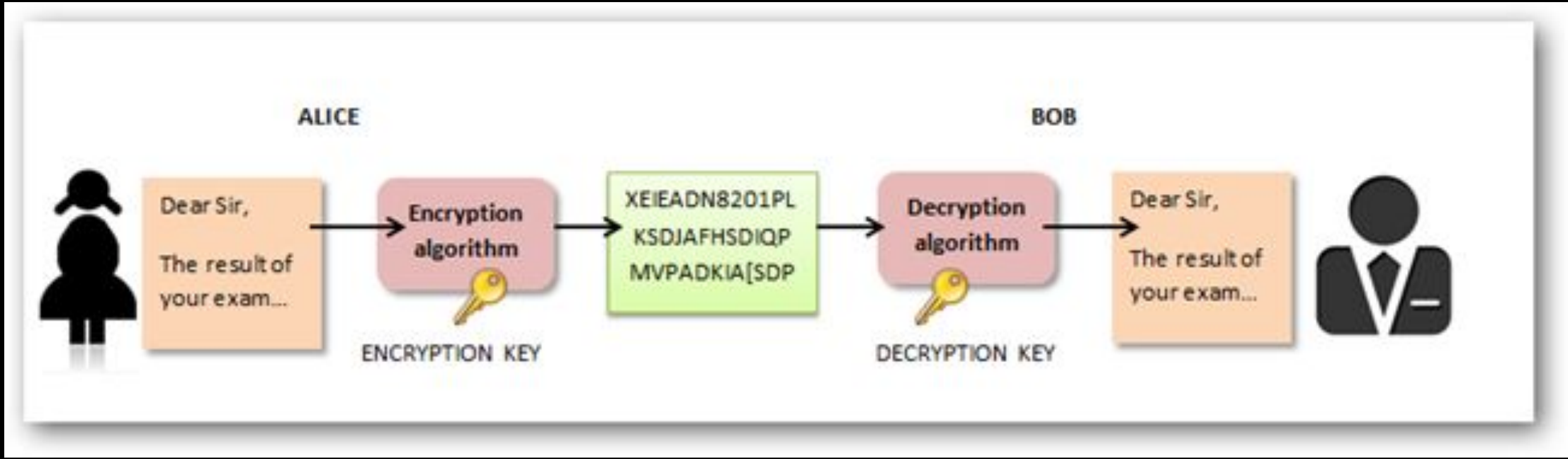
Encryption

Types of encryption:

- Symmetric key algorithms use related or identical encryption keys for both encryption and decryption.
- Asymmetric key algorithms use different keys for encryption and decryption—this is usually referred to as Public-key Cryptography.

Encryption

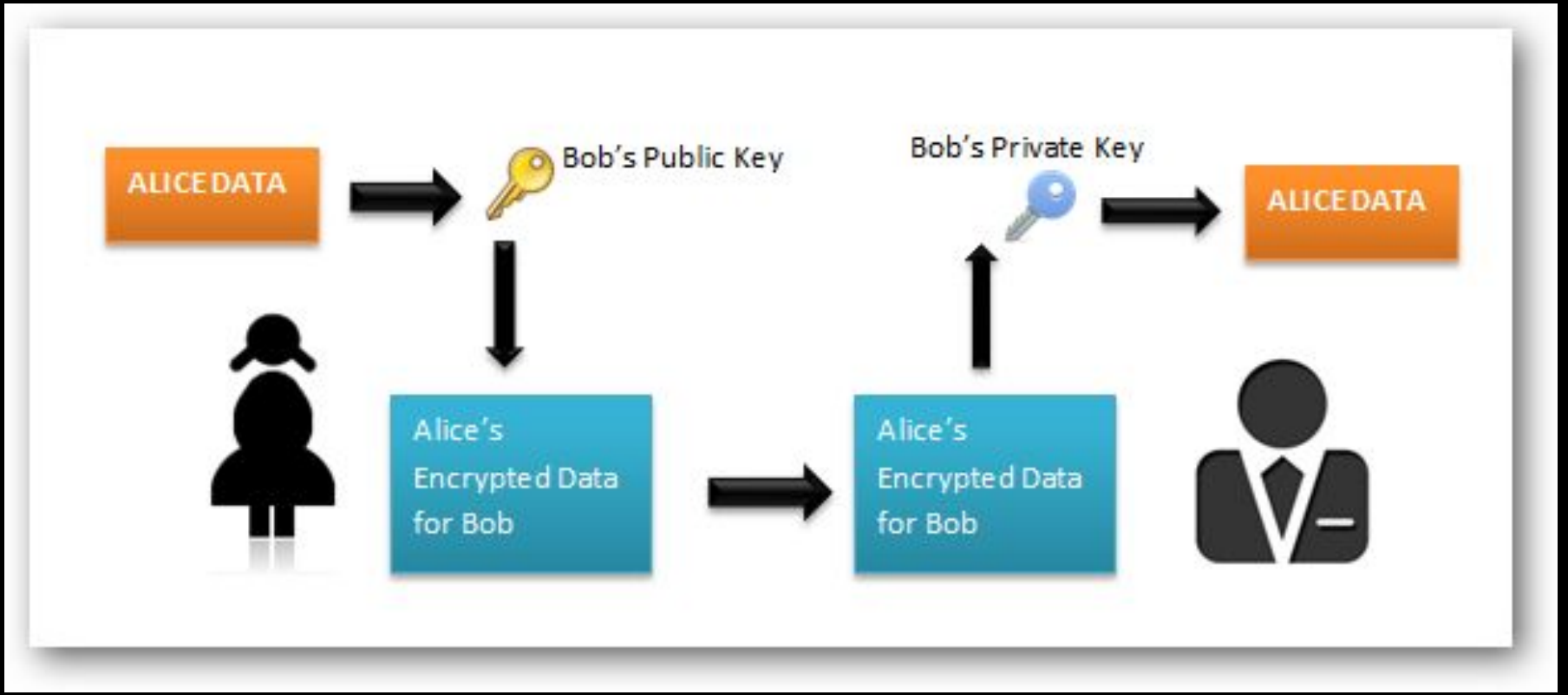
Symmetric key encryption: like Postal concept



Example: Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, TDES, and IDEA.

Encryption

Asymmetric key encryption



Examples: RSA , DIFFIE, ELLIPTICAL KEY.

Encryption

Asymmetric | Public key encryption:

- Involves use of 2 separate keys (private key & public key)
- Private key is kept secret, Public key is made public for others.

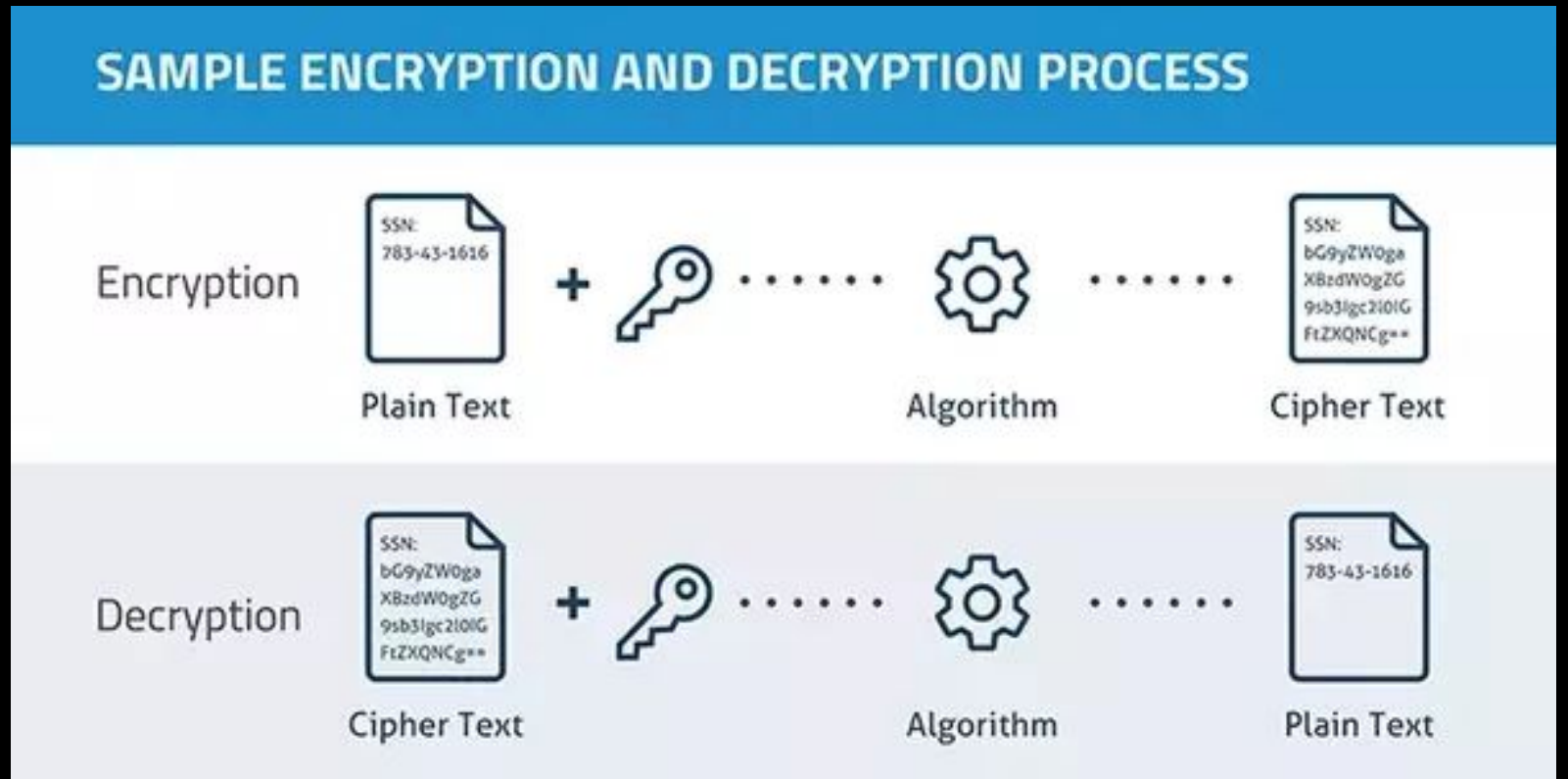
6 factors to be considered.

1. Plain text: readable data fed as input to algorithm
2. Encryption algorithm: Performs various mathematical transformations on plaintext.
3. Public keys and
4. Private keys: Among these two keys, one is used for encryption and other for decryption.

Encryption

5. Cipher text: scrambled message produced as output. It depends on plaintext & key. For a given message, two different keys will produce two different cipher texts.

6. Decryption algorithm: This algorithm accepts the cipher text and the matching key & then produces the original plaintext.



Encryption

Steps:

- Each user generates a pair of keys to be used for encryption & decryption of messages.
- Each user places one of two keys in public register. This is public key. The companion key is kept private.
- If a sender wishes to send a private message to a receiver, sender encrypts message using receiver's public key.
- When receiver receives the message, he decrypts it using receiver's private key. No other recipient can decrypt the message because only the receiver knows his private key.

Thank you.