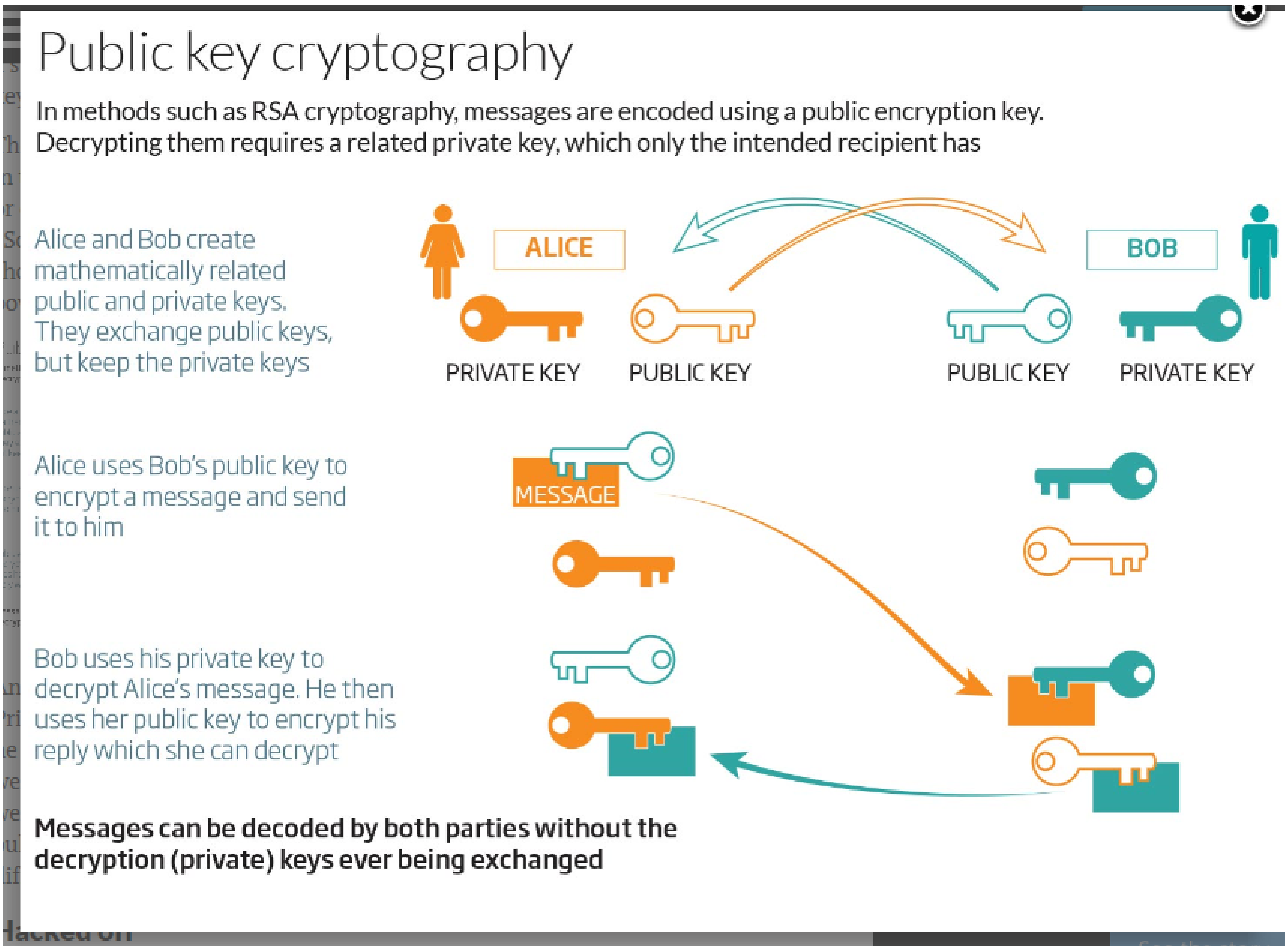

Public key cryptography

In methods such as RSA cryptography, messages are encoded using a public encryption key. Decrypting them requires a related private key, which only the intended recipient has

Alice and Bob create mathematically related public and private keys. They exchange public keys, but keep the private keys

Alice uses Bob's public key to encrypt a message and send it to him

Bob uses his private key to decrypt Alice's message. He then uses her public key to encrypt his reply which she can decrypt

Messages can be decoded by both parties without the decryption (private) keys ever being exchanged

Hacked off