Lancashire
Cyber Foundry

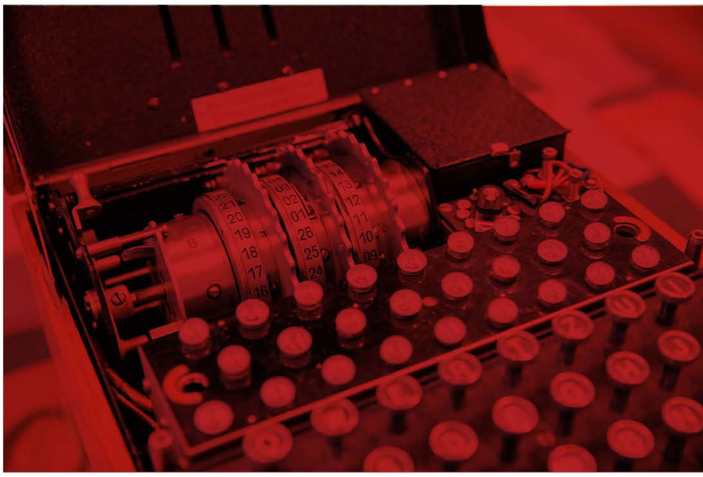
What are Public/Private Keys?

READ TIME: 2 MINS

AUDIENCE: BUSINESS & TECHNOLOGY

Public/private key pairs are used for public-key cryptography, also known as asymmetric cryptography.

In comparison to its less modern counterpart – symmetric cryptography – asymmetric cryptography uses two distinct keys for encryption and decryption. Asymmetric cryptography is the current industry standard for encryption due to its nature of requiring two keys, and because it requires a 2048-bit or longer key size, which means cracking the encryption is highly infeasible. For a 2048-bit key, there would be 22048 possible combinations, which would take modern computers around 300 trillion years to crack.



For asymmetric cryptography, a private key is generated along with its corresponding public key. This means that the public key and private key are mathematically similar, however a private key cannot be generated from a public key. The 'public key' is the key a party would share to allow other parties to send them encrypted messages, with no security risk if the key is shared publicly. The 'private key' is the key a party would keep to themselves, with an extreme security risk if it were to be made public or leaked. Messages encrypted with a public key can only be decrypted using the corresponding private key, and the private key can only decrypt messages encrypted with its corresponding public key. One example use case of a public/private key pair would be email transfer. When sending an email to a recipient, their public key is used to encrypt the outgoing email so that only the recipient, who holds the corresponding private key, can decrypt and read the contents of the email. Of course, this entire process is handled automatically by the emailing software.

European Union
European Regional
Development Fund

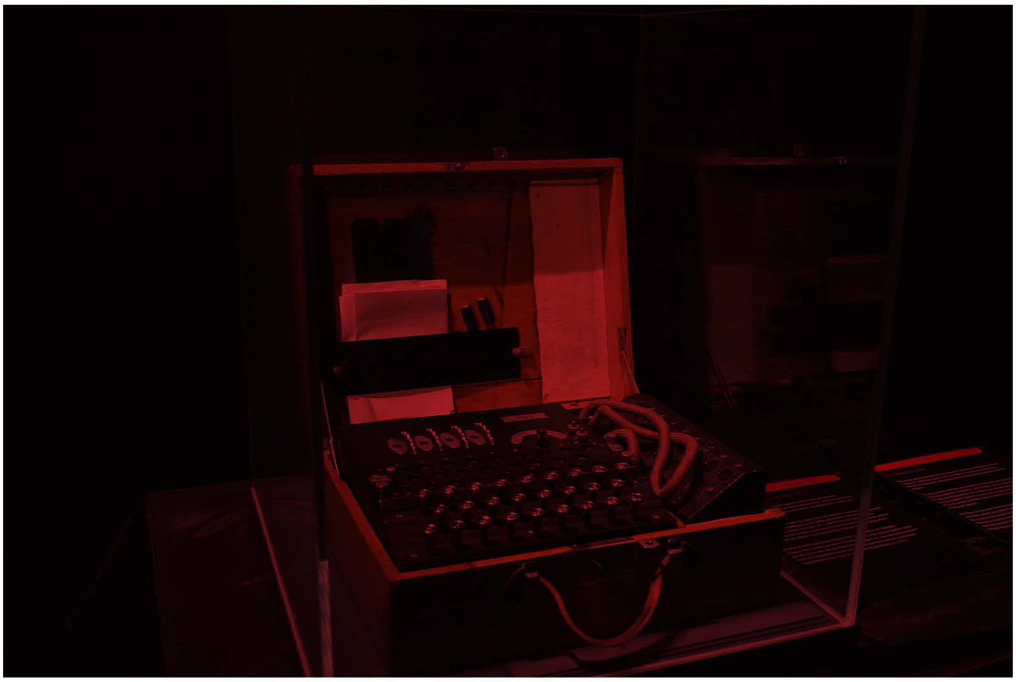
NORTHERN POWERHOUSE HM Government

Lancaster University

Public/Private Key Pairs

Asymmetric encryption also enables the use of digital signatures, where the sender uses a signing algorithm to produce a signature from a private key and a desired message, from which the recipient uses a signature verifying algorithm along with the sender's message and the private key's corresponding public key to verify the sender's signature. An example use case of digital signatures would be in videogame systems such as the PS3, where every PS3 contains a public key for software update verification. When Sony sends out a PS3 software update, the updates are signed using a private key which only Sony has access to. A PS3 receiving an update would use the public key to verify the contents of the update, preventing unofficial software updates from being installed.

WRITTEN BY HUSSAIN HAMIDI - LCF INTERN



ABOUT US

Lancashire Cyber Foundry

The Lancashire Cyber Foundry runs a programme designed to s upport businesses facing cyber challenges in Lancashire. Digital Innovation support is part of this programme but there is also business strategy support available which includes specialised workshops to help businesses innovate and grow.

To find out more visit our website, https://www.lancashirecyberfoundry.co.uk/ or email us at;

cyberfoundry@lancaster.ac.uk