(1) What is Public Key Cryptography?

Public Key Cryptography (PKC) forms the backbone of many secure communication protocols, including Secure Sockets Layer (SSL), Transport Layer Security (TLS), and many others.

At its core, PKC is an asymmetric encryption system. This means that it uses two different keys for encryption and decryption. You have a public key that you can freely distribute and a private key that you must keep secret. Anyone can use your public key to encrypt a message, but only you with your private key can decrypt it.

ما هو تشفير المفتاح العام؟

يشكل تشفير المفتاح العام (PKC) العمود الفقري للعديد من بروتوكولات الاتصال الآمنة، بما في ذلك طبقة المقابس الآمنة (SSL) وأمن طبقة النقل (TLS) وغيرها الكثير.

في جوهره، PKCهو نظام تشفير غير متماثل. وهذا يعني أنه يستخدم مفتاحين مختلفين للتشفير وفك التشفير. لديك مفتاح عام يمكنك توزيعه بحرية ومفتاح خاص يجب عليك الحفاظ على سريته. يمكن لأي شخص استخدام مفتاحك العمومي لتشفير رسالة، ولكنك وحدك بمفتاحك الخاص يمكنك فك تشفيرها.

(2) How does public-private key encryption work?

Now, let's go a little further. When someone wants to send you a secure message, they will encrypt it using your public key, creating a ciphertext that only the owner of the private key can decrypt. This way, even if someone intercepts the message, they won't be able to decrypt it without your private key.

However, it's not just for encrypting messages. You can turn the process around for digital signatures – a way to ensure that the message hasn't been tampered with. You'll use your private key to encrypt the message or a hashed version of it. Then, anyone can verify its authenticity by decrypting the signature using your public key.

Key management can be complicated, and there's a risk of losing or stealing your private key, compromising your security. So, it's important to handle your keys carefully.

كيف يعمل تشفير المفتاح العام والخاص؟

والآن، دعنا نذهب أبعد من ذلك قليلاً. عندما يريد شخص ما أن يرسل لك رسالة آمنة، سيقوم بتشفيرها باستخدام مفتاحك العام، مما يؤدي إلى إنشاء نص مشفر لا يستطيع فك تشفيره إلا صاحب المفتاح الخاص. وبهذه الطريقة، حتى لو اعترض شخص ما الرسالة، فلن يتمكن من فك تشفيرها بدون مفتاحك الخاص.

ومع ذلك، فهي ليست فقط لتشفير الرسائل. يمكنك قلب العملية للتوقيعات الرقمية – وهي طريقة لضمان عدم التلاعب بالرسالة. ستستخدم مفتاحك الخاص لتشفير الرسالة أو نسخة مجزأة منها. بعد ذلك، يمكن لأي شخص التحقق من صحته عن طريق فك تشفير التوقيع باستخدام مفتاحك العام.

يمكن أن تكون إدارة المفاتيح أمرًا معقدًا، وهناك خطر فقدان مفتاحك الخاص أو سرقته، مما يعرض أمنك للخطر. لذلك، من الضروري أن تتعامل مع مفاتيحك بعناية.

(3) How does TLS/SSL use public key encryption?

Now that you know how PKC works, let's see how protocols like TLS/SSL implement this method for secure transmission. TLS/SSL, or Transport Layer Security and its predecessor Secure Sockets Layer, are encryption protocols designed to provide secure communication over a computer network. They use public key encryption, specifically asymmetric encryption, to achieve this. SSL is now deprecated, with TLS becoming the standard.

When a client connects to a TLS-secured server, the server shares its public key with the client to establish an encrypted connection using digital certificates containing the server's public key and identity. The client uses this public key to encrypt and send a secret key to the server.

This is where the private key of the SSL certificate comes in. The server uses its private key to decrypt the secret key sent by the client. This pair of keys – the public and private keys – are uniquely linked. Anything encrypted with the public key can only be decrypted by the corresponding private key.

Once the secret key is decrypted, both the server and the client have a shared secret key. This key is then used to symmetrically encrypt the data sent between them during that session.

Basically, TLS/SSL uses asymmetric encryption for the initial handshake to securely create a symmetric key. This symmetric key is then used to encrypt the data in bulk. This combination of asymmetric and symmetric encryption ensures a secure and efficient connection.

كيف يستخدم TLS/SSL تشفير المفتاح العام؟

والآن بعد أن تعرفت على كيفية عملPKC ، دعنا نرى كيف تطبق بروتوكولات مثل TLS/SSLهذه الطريقة للإرسال الآمنTLS/SSL .، أو أمن طبقة النقل (Transport Layer Security)وسابقهSecure Sockets Layer ، هما بروتوكولات تشفير مصممة لتوفير اتصال آمن عبر شبكة الكمبيوتر. وهي تستخدم تشفير المفتاح العام، وتحديداً التشفير غير المتماثل، لتحقيق ذلك. تم إهمال SSL الآن، حيث أصبحت TLS هي المعيار.

عندما يتصل العميل بخادم مؤمن باستخدامTLS ، يشارك الخادم مفتاحه العام مع العميل لإنشاء اتصال مشفر باستخدام شهادات رقمية تحتوي على المفتاح العام وهوية الخادم. يستخدم العميل هذا المفتاح العام لتشفير وإرسال مفتاح سري إلى الخادم.

هنا يأتي دور المفتاح الخاص لشهادة .SSL يستخدم الخادم مفتاحه الخاص لفك تشفير المفتاح السري الذي أرسله العميل. زوج المفاتيح هذا – المفاتيح العامة والخاصة – مرتبطان بشكل فريد. أي شيء مشفر بالمفتاح العام لا يمكن فك تشفيره إلا بواسطة المفتاح الخاص المقابل.

بمجرد فك تشفير المفتاح السري، يكون لدى كل من الخادم والعميل مفتاح سري مشترك. ثم يتم استخدام هذا المفتاح للتشفير المتماثل للبيانات المرسلة بينهما خلال تلك الجلسة.

في الأساس، يستخدم TLS/SSL تشفيرًا غير متماثل للمصافحة الأولية لإنشاء مفتاح متماثل بشكل آمن. ثم يتم استخدام هذا المفتاح المتماثل لتشفير البيانات بالجملة. هذا المزيج من التشفير غير المتماثل والمتماثل يضمن اتصالاً آمناً وفعالاً.

(4) What is public key encryption and how does it work?

Now that you have a good understanding of how TLS/SSL uses private and public keys, let's take a look at public key encryption.

Public key encryption, also known as asymmetric encryption, is a method of encrypting data using a pair of keys.

Here's how public encryption works: A public key encrypts sensitive data, and anyone can use it to encrypt the information. A private key, on the other hand, is secret and only the owner knows it. This private key decrypts the data encrypted with the corresponding public key.

For example, if Alice wanted to send sensitive information to Bob, she would encrypt it using Bob's public key. Bob would then use his private key to decrypt the received data. Even if someone intercepted the information, they wouldn't be able to read it without Bob's matching private key.

Public key encryption uses a process called key pair generation. The two keys are mathematically related – what one key encrypts can only be decrypted by the other key.

Public key encryption secures communications over the Internet, including email and online banking transactions. The most common public key encryption algorithms include RSA (RSA) and ECC (Elliptic Curve Cryptography).

ما هو تشفير المفتاح العام وكيف يعمل؟

والآن بعد أن أصبحتَ على دراية جيدة بكيفية استخدام TLS/SSL للمفاتيح الخاصة والعامة، دعنا نلقي نظرة على تشفير المفتاح العام.

تشفير المفتاح العام، المعروف أيضًا باسم التشفير غير المتماثل، هو طريقة لتشفير البيانات باستخدام زوج من المفاتيح.

إليك كيفية عمل التشفير العام: يقوم المفتاح العام بتشفير البيانات الحساسة، ويمكن لأي شخص استخدامه لتشفير المعلومات. من ناحية أخرى، يكون المفتاح الخاص سريًا ولا يعرفه سوى المالك فقط. يقوم هذا المفتاح الخاص بفك تشفير البيانات المشفرة بالمفتاح العام المقابل.

على سبيل المثال، إذا أرادت أليس إرسال معلومات حساسة إلى بوب، فستقوم بتشفيرها باستخدام المفتاح العام لبوب. سيستخدم بوب بعد ذلك مفتاحه الخاص لفك تشفير البيانات المستلمة. حتى إذا اعترض شخص ما المعلومات، فلن يتمكن من قراءتها بدون مفتاح بوب الخاص المطابق.

يستخدم تشفير المفتاح العام عملية تسمى توليد زوج المفاتيح. كلا المفتاحين مرتبطان رياضيًا – ما يشفره أحد المفتاحين لا يستطيع فك تشفيره إلا المفتاح الآخر.

يعمل تشفير المفتاح العام على تأمين الاتصالات عبر الإنترنت، بما في ذلك رسائل البريد الإلكتروني والمعاملات المصرفية عبر الإنترنت. تتضمن أكثر خوارزميات تشفير المفتاح العام شيوعًا خوارزميات تشفير المفتاح العام (RSA) RSA و ECC (تشفير المنحنى الإهليلجي).

(5) What is private key encryption and how does it work?

Private key encryption is a different process compared to public key encryption. This method involves only one key that is used for both encryption and decryption.

In private key encryption, also known as symmetric encryption, you will use the same key to encrypt and decrypt data. It's like locking and unlocking a personal safe with the same key. Here's how it works: Let's say you have a message that needs to be encrypted. You will apply the private key to this plaintext using an encryption algorithm to convert it into an unreadable form called ciphertext.

This ciphertext can only be decrypted by re-encrypting the plaintext using the same private key. Any third party who doesn't have the private key will not be able to decrypt the message, ensuring that it remains confidential.

However, the challenge lies in sharing the private key securely between users. If it is intercepted, an unauthorized third party can decrypt any encrypted messages. As such, private key encryption is primarily used in secure environments where key distribution is not an issue.

ما هو تشفير المفتاح الخاص وكيف يعمل؟

تشفير المفتاح الخاصهو عملية مختلفة مقارنة بتشفير المفتاح العام. تتضمن هذه الطريقة مفتاحًا واحدًا فقط يُستخدم لكل من التشفير وفك التشفير.

في تشفير المفتاح الخاص، المعروف أيضًا باسم التشفير المتماثل، ستستخدم نفس المفتاح لتشفير البيانات وفك تشفيرها. الأمر يشبه قفل وفتح خزنة شخصية بنفس المفتاح. إليك كيفية عملها: لنفترض أن لديك رسالة تحتاج إلى تشفيرها. ستطبّق المفتاح الخاص على هذا النص العادي باستخدام خوارزمية تشفير لتحويله إلى صيغة غير قابلة للقراءة تُسمى النص المشفر.

لا يمكن فك تشفير هذا النص المشفر إلا بإعادة تشفير النص العادي باستخدام نفس المفتاح الخاص. لن يتمكن أي طرف ثالث لا يملك المفتاح الخاص من فك تشفير الرسالة، مما يضمن بقاءها سرية.

ومع ذلك، يكمن التحدي في مشاركة المفتاح الخاص بأمان بين المستخدمين. إذا تم اعتراضها، يمكن لطرف ثالث غير مصرح له فك تشفير أي رسائل مشفرة. على هذا النحو، يتم استخدام تشفير المفتاح الخاص بشكل أساسي في البيئات الآمنة حيث لا يمثل توزيع المفاتيح مشكلة.

(6) What is the difference between a public key and a private key?

You may be wondering what separates a public key from a private key.

As you know, a public key is used for encryption and is freely shared, whereas a private key, which is kept secure and secret, is used for decryption. Let's explore other differences between private key encryption vs. public key encryption.

ما الفرق بين المفتاح العام والمفتاح الخاص؟

قد تتساءل عما يميز المفتاح العام عن المفتاح الخاص.

كما تعلم، يتم استخدام المفتاح العام للتشفير ويتم مشاركته بحرية، في حين يتم استخدام المفتاح الخاص، الذي يتم الاحتفاظ به آمنًا وسريًا، لفك التشفير. دعونا نستكشف الاختلافات الأخرى بين تشفير المفتاح الخاص مقابل تشفير المفتاح العام.

Security of Private Keys

The security of your private key is crucial because it is the only means of decrypting messages encrypted with your public key. Private keys are long strings of numbers and letters from a mathematical algorithm. They are unique and impossible to duplicate.

In contrast, a public key is derived from the private key and can be shared publicly. Although you can learn the private key from the public key, it is practically impossible because it would take a long time with today's computers. So, keep your private keys secure and hidden from anyone trying to snoop.

If someone gains access to your private keys, they effectively control your encrypted data. It is essential to understand this distinction to maintain strong security protocols.

أمان المفاتيح الخاصة

إن أمان مفتاحك الخاص أمر بالغ الأهمية لأنه الوسيلة الوحيدة لفك تشفير الرسائل المشفرة بمفتاحك العام. المفاتيح الخاصة عبارة عن سلاسل طويلة من الأرقام والحروف من خوارزمية رياضية. إنها فريدة من نوعها ومن المستحيل تكرارها.

في المقابل، يُشتق المفتاح العام من المفتاح الخاص ويمكن مشاركته علانية. على الرغم من أنه يمكنك معرفة المفتاح الخاص من المفتاح العام، إلا أن ذلك مستحيل عملياً لأنه سيستغرق وقتاً طويلاً مع أجهزة الكمبيوتر الحالية. لذا، احتفظ بمفاتيحك الخاصة آمنة ومخفية عن أي شخص يحاول التطفل.

إذا تمكن شخص ما من الوصول إلى مفاتيحك الخاصة، فإنه يتحكم بفعالية في بياناتك المشفرة. من الضروري فهم هذا التمييز للحفاظ على بروتوكولات أمان قوية.

Emphasizing the Differences Between Public Key and Private Key

Although both keys are integral to encryption, there are several fundamental differences that set public and private keys apart.

In symmetric key encryption, the same key is used for encryption and decryption. However, with public and private keys, there are two keys.

The public key is like a front door, open to anyone to encrypt messages, while the private key is the trusted carrier, only you have it to decrypt.

The decryption process requires checking whether the received message matches the digital signature standard. If the signature matches, only the intended recipient can decrypt it.

With initial analysis, the private key becomes a secret key, and with elliptic curve encryption, it can generate digital signatures.

The key agreement results in a shared secret key, which ensures that messages encrypted only according to the Federal Information Processing Standards are valid.

التأكيد على اختلافات المفتاح العام والمفتاح الخاص المختلفة

على الرغم من أن كلا المفتاحين جزء لا يتجزأ من التشفير، إلا أن هناك العديد من الاختلافات الجوهرية التي تميز المفاتيح العامة والخاصة عن بعضها البعض.

في التشفير بالمفتاح المتماثل، يتم استخدام نفس المفتاح للتشفير وفك التشفير. ومع ذلك، مع المفاتيح العامة والخاصة، هناك مفتاحان.

المفتاح العام هو بمثابة الباب الأمامي، مفتوح لأي شخص لتشفير الرسائل، بينما المفتاح الخاص هو الناقل الموثوق به، أنت فقط من يحمله لفك التشفير.

تتطلب عملية فك التشفير التحقق مما إذا كانت الرسالة المستلمة تتطابق مع معيار التوقيع الرقمي. إذا تطابق التوقيع، يمكن للمستلم المقصود فقط فك تشفيره.

مع التحليل الأولي، يصبح المفتاح الخاص مفتاحًا سريًا، ومع تشفير المنحنى الإهليلجي، يمكن أن يولد توقيعات رقمية.

تؤدي اتفاقية المفتاح إلى مفتاح سري مشترك، مما يضمن صلاحية الرسائل المشفرة فقط وفقًا لمعايير معالجة المعلومات الفيدرالية.

(7) What are some examples of uses for public key and private key encryption?

Let's look at three basic examples: secure email communications, cryptocurrency transactions, and website authentication.

ما هي بعض الأمثلة على استخدامات تشفير المفتاح العام والمفتاح الخاص؟

لننظر في ثلاثة أمثلة أساسية: اتصالات البريد الإلكتروني الآمنة، ومعاملات العملات الرقمية، والمصادقة على المواقع الإلكترونية.

Secure Email Communications

In securing your email communications, there are two primary uses for public key and private key encryption.

First, these keys ensure confidentiality. When you send an email, it is encrypted with the recipient's public key and only one private key can decrypt it. If a hacker intercepts the email, they won't be able to read it without the corresponding private key.

Second, the keys provide authentication and non-repudiation. When you sign an email with your private key, the recipient can use your public key to verify that it was actually you who sent it. Furthermore, you can't refuse to send the email because only you have access to your private key.

These encryption methods secure emails, protecting sensitive information from unauthorized access and tampering.

اتصالات البريد الإلكتروني الآمنة

في تأمين اتصالات البريد الإلكتروني الخاص بك، هناك استخدامان أساسيان لتشفير المفتاح العام والمفتاح الخاص.

أولاً، تضمن هذه المفاتيح السرية. عندما ترسل بريدًا إلكترونيًا، يتم تشفيره بالمفتاح العام للمستلم ويمكن لمفتاح خاص واحد فقط فك تشفيره. إذا اعترض أحد المخترقين البريد الإلكتروني، فلن يتمكنوا من قراءته دون المفتاح الخاص المقابل.

ثانياً، توفر المفاتيح المصادقة وعدم التنصل. عندما تقوم بتوقيع رسالة بريد إلكتروني باستخدام مفتاحك الخاص، يمكن للمستلم استخدام مفتاحك العام للتحقق من أنك أنت من أرسلتها بالفعل.

وعلاوة على ذلك، لا يمكنك رفض إرسال البريد الإلكتروني لأنك أنت فقط من يمكنه الوصول إلى مفتاحك الخاص.

تعمل طرق التشفير هذه على تأمين رسائل البريد الإلكتروني، وحماية المعلومات الحساسة من الوصول غير المصرح به والتلاعب بها.

Website Authentication

A website's server creates a pair of keys: one private, which is kept secret, and one public, which is shared with your browser. Your browser then encrypts your password using this public key. Only the server, with its private key, can decrypt and verify the password.

Another example of public key encryption is TLS, which is used to secure data transmission between your browser and a website. A website's SSL certificate contains a public key. Your browser uses this key to encrypt data sent to the website, which only the website's private key can decrypt, ensuring the privacy and integrity of the data.

مصادقة الموقع الإلكتروني

ينشئ خادم الموقع زوجاً من المفاتيح: واحد خاص، يبقى سراً، والآخر عام تتم مشاركته مع متصفحك. ثم يقوم متصفحك بتشفير كلمة المرور الخاصة بك باستخدام هذا المفتاح العام. لا يستطيع سوى الخادم، بمفتاحه الخاص، فك تشفير كلمة المرور والتحقق منها.

مثال آخر على تشفير المفتاح العام هوTLS ، الذي يُستخدم لتأمين نقل البيانات بين المتصفح وموقع الويب. تحتوي شهادة SSL الخاصة بالموقع على مفتاح عام. يستخدم المتصفح الخاص بك هذا المفتاح لتشفير البيانات المرسلة إلى الموقع، والتي لا يستطيع فك تشفيرها إلا المفتاح الخاص بالموقع، مما يضمن خصوصية البيانات وسلامتها.

Cryptocurrency Transactions

In this digital economy, your public key is like your bank account number. It is an address where others can send cryptocurrency. However, your private key is like your secret PIN or password, allowing you to access and manage your funds.

For example, when you transact with Bitcoin, you sign the transaction using your private key, which is then publicly verified using your public key. This cryptographic signature proves that you are the rightful owner of the funds.

معاملات العملات المشفرة

في هذا الاقتصاد الرقمي، يكون مفتاحك العام شبيهاً برقم حسابك المصرفي. إنه عنوان يمكن للآخرين إرسال العملات الرقمية إليه. ومع ذلك، فإن المفتاح الخاص يشبه رقم التعريف الشخصي السري أو كلمة المرور السرية الخاصة بك، مما يسمح لك بالوصول إلى أموالك وإدارتها.

على سبيل المثال، عندما تقوم بالتعامل بالبيتكوين، فإنك تقوم بتوقيع المعاملة باستخدام مفتاحك الخاص، والذي يتم التحقق منه بعد ذلك بشكل عام باستخدام مفتاحك العام. يثبت هذا التوقيع المشفر أنك المالك الشرعي للأموال.

(8) Frequently Asked Questions

Is public key encryption asymmetric or symmetric?

Public key encryption is asymmetric because it uses key pairs. The public key is shared publicly, allowing anyone to encrypt messages, while the private key is kept secret and used for decryption.

الأسئلة الشائعة

هل تشفير المفتاح العام غير متماثل أم متماثل؟

تشفير المفتاح العام غير متماثل لأنه يستخدم أزواج مفاتيح. تتم مشاركة المفتاح العام بشكل علني، مما يسمح لأي شخص بتشفير الرسائل، بينما يتم الاحتفاظ بالمفتاح الخاص سراً ويُستخدم لفك التشفير.

What is another name for public key encryption?

Another name for public key encryption is asymmetric encryption, as it involves a pair of keys, one for encryption (the public key) and one for decryption (the private key), providing a different approach than symmetric encryption where the same key is used for both encryption and decryption

ما هو الاسم الآخر لتشفير المفتاح العام؟

هناك اسم آخر لتشفير المفتاح العام وهو التشفير غير المتماثل، حيث أنه يتضمن زوجًا من المفاتيح، أحدهما للتشفير (المفتاح العام) والآخر لفك التشفير (المفتاح الخاص)، مما يوفر نهجًا مختلفًا عن التشفير المتماثل حيث يتم استخدام نفس المفتاح لكل من التشفير وفك التشفير

Is public key encryption secure?

Yes, public key encryption is secure because it uses a pair of keys, while keeping the private key secret. Security is based on the difficulty of deriving the private key from the public key

هل تشفير المفتاح العام آمن؟

نعم، يعتبر تشفير المفتاح العام آمنًا بسبب استخدامه لزوج من المفاتيح، مع الحفاظ على سرية المفتاح الخاص. يعتمد الأمان على صعوبة استخلاص المفتاح الخاص من المفتاح العام

Is the public key a number?

A public key is a large number that results from complex mathematical calculations. Specifically, it is derived from mathematical algorithms involving prime numbers, making it difficult to reverse engineer the private key from the public key.

هل المفتاح العام رقم؟

المفتاح العام هو رقم كبير ينتج عن عمليات حسابية معقدة. على وجه التحديد، فهي مشتقة من خوارزميات رياضية تتضمن أعدادًا أولية، مما يجعل من الصعب عكس هندسة المفتاح الخاص من المفتاح العام.

Where is the private key stored?

The private key is securely stored on the owner's device, on a server, or in a designated key management system.

أين يتم تخزين المفتاح الخاص؟

يتم تخزين المفتاح الخاص بشكل آمن على جهاز المالك، أو على الخادم، أو في نظام إدارة مفاتيح معين.

Can I share my public key?

Yes, sharing your public key is a standard and secure practice. Your public key is designed for distribution and allows others to encrypt messages or verify digital signatures associated with your private key.

هل يمكنني مشاركة المفتاح العام الخاص بي؟

نعم، تعد مشاركة مفتاحك العام ممارسة قياسية وآمنة. مفتاحك العام مصمم للتوزيع ويسمح للآخرين بتشفير الرسائل أو التحقق من التواقيع الرقمية المرتبطة بمفتاحك الخاص.

How are public and private keys created?

Public and private keys are created using mathematical algorithms, often involving complex operations with prime numbers. The public key is derived from the private key, and the two are created together as a pair to ensure the mathematical relationship between them.

كيف يتم إنشاء المفاتيح العامة والخاصة؟

يتم إنشاء المفاتيح العامة والخاصة باستخدام خوارزميات رياضية، وغالبًا ما تتضمن عمليات معقدة باستخدام الأعداد الأولية. يتم اشتقاق المفتاح العام من المفتاح الخاص، ويتم إنشاء كلاهما معًا كزوج لضمان العلاقة الرياضية بينهما.

(9) Conclusion

In short, understanding public key cryptography vs. private key cryptography is all about knowing the difference between public and private keys. A public key encrypts information, while a private key decrypts information.

In the dynamic cybersecurity space, the practical implications of public and private keys are ubiquitous. PKC powers secure web browsing and file transfers. It protects blockchain transactions and email communications. Remember, store your private keys in a secure location, and your sensitive data will not fall into the hands of attackers.

الخاتمة

باختصار، إن فهم تشفير المفاتيح العامة مقابل تشفير المفاتيح الخاصة يتعلق بمعرفة الفرق بين المفاتيح العامة والخاصة. يقوم المفتاح العام بالتشفير، بينما يقوم المفتاح الخاص بفك تشفير المعلومات.

في مجال الأمن الديناميكي عبر الإنترنت، فإن الآثار العملية للمفاتيح العامة والخاصة موجودة في كل مكان. يعمل PKC على تشغيل تصفح الويب الآمن ونقل الملفات. فهو يحمي معاملات البلوك تشين والاتصالات عبر البريد الإلكتروني. تذكّر، قم بتخزين مفاتيحك الخاصة في مكان آمن، ولن تقع بياناتك الحساسة في أيدي المهاجمين.