

SSL, TLS and HTTPS



- SSL: Secure Sockets Layer (deprecated)
- TLS: Transport Layer Security (successor to SSL)
- Can be used to provide secure web browsing with HTTPS (can also be used with other applications such as email)

SSL, TLS and HTTPS (Cont.)



- Uses symmetric cryptography to encrypt transmitted data
- Symmetric keys are generated uniquely for each connection
- Authentication is provided by public key cryptography
- Message Authentication Code provides integrity

HTTPS Example



HTTPS Example



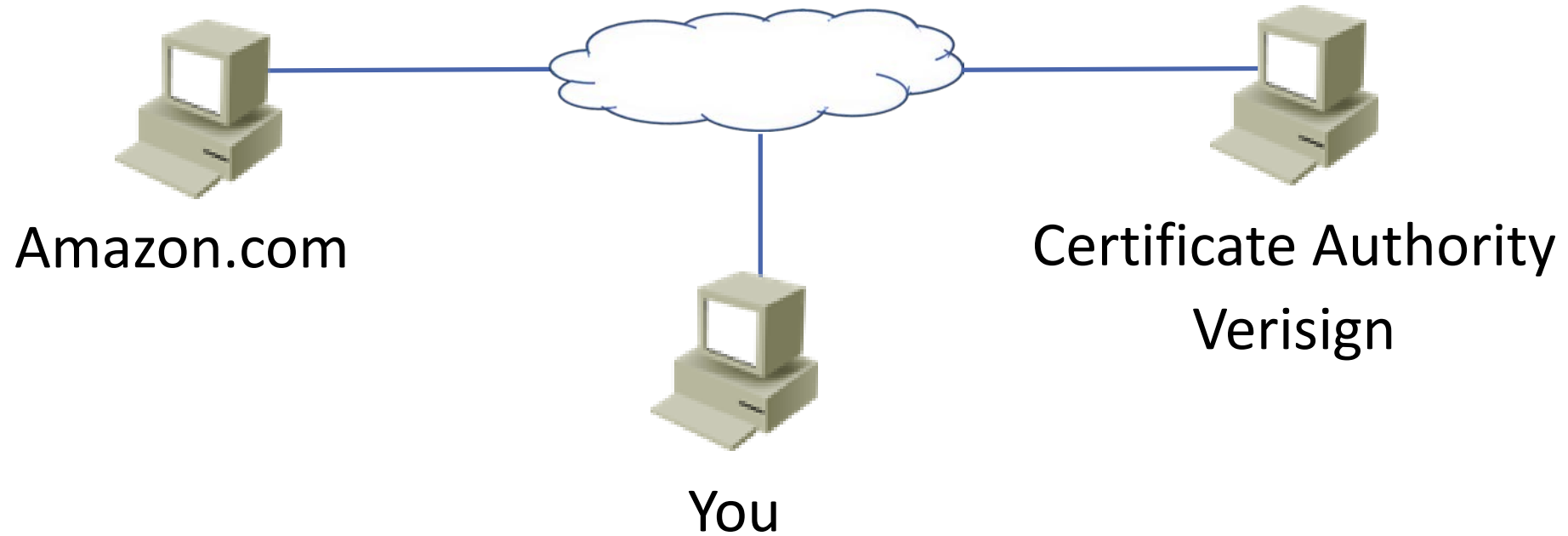
Out of band verification
"Prove you're really Amazon.com"

HTTPS Example



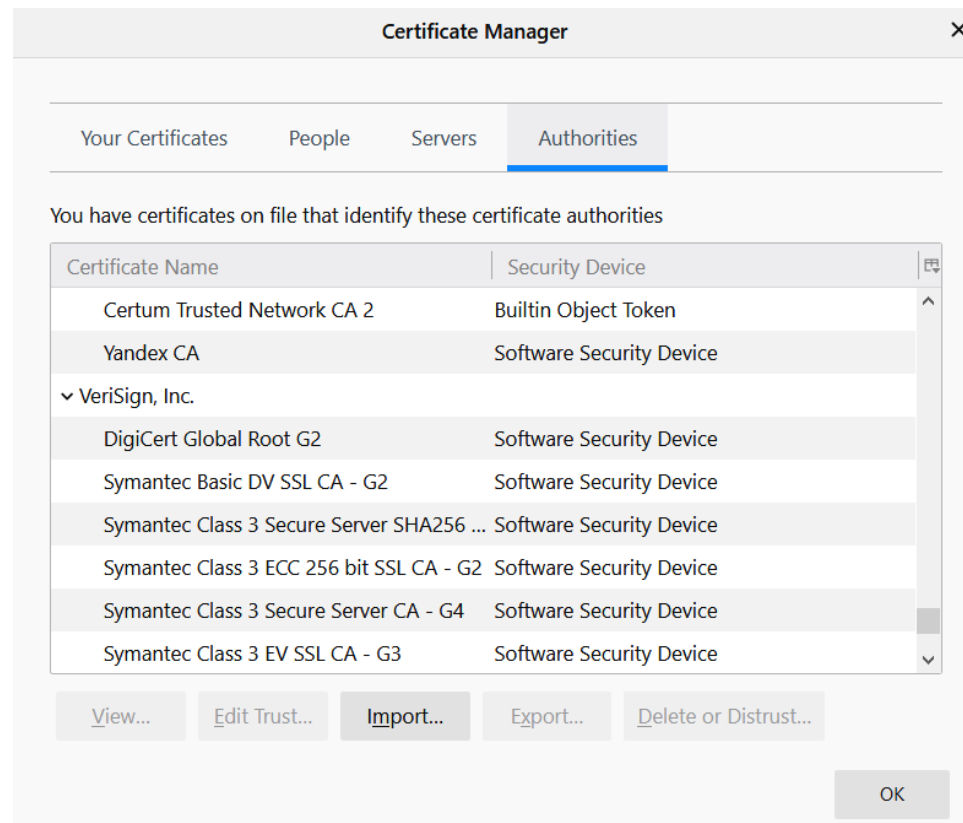
Certificate
Website: <https://www.amazon.com>
Amazon's public key
Signed by Verisign's private key

HTTPS Example



HTTPS Example

- Your web browser trusts the public Certificate Authorities and has a copy of their public keys
- Firefox:



HTTPS Example



HTTPS Example



HTTPS Example



- Your browser trusts Verisign and has its public key (that information is installed with your web browser)
- It checks the certificate with Verisign's public key
- Verisign is the only entity with their private key, so if it checks out it must have been signed by Verisign and you trust the certificate
- You now know that who you are communicating with has sent you the valid certificate for Amazon.com...

HTTPS Example

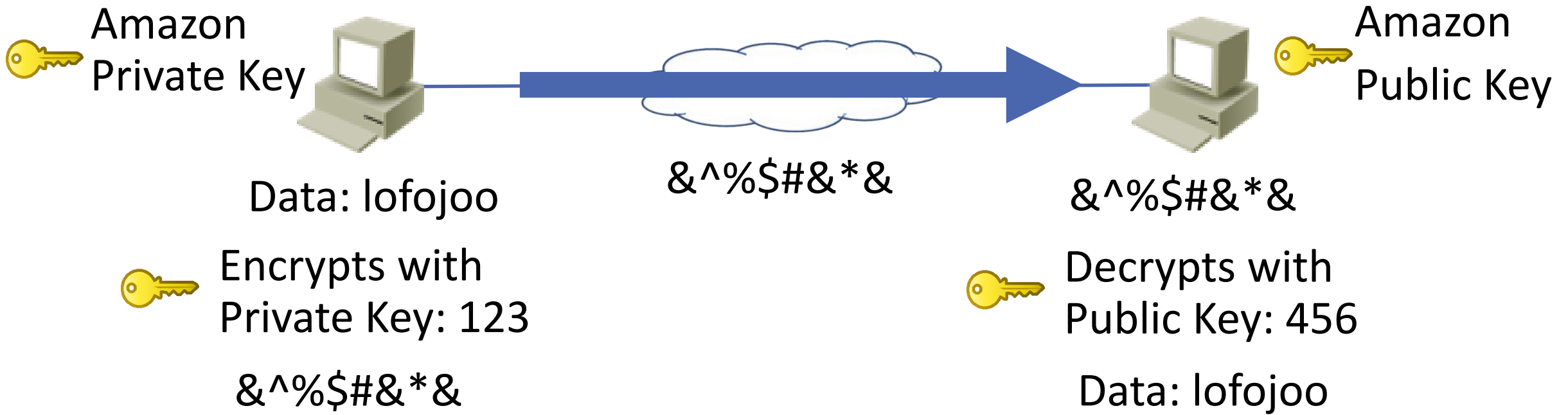


- But you don't know that you are communicating with Amazon.com yet!
- Anybody could have sent you the valid certificate for Amazon.com and be pretending to be them
- You have not authenticated them yet

HTTPS Example



Asymmetric Encryption - Confidentiality



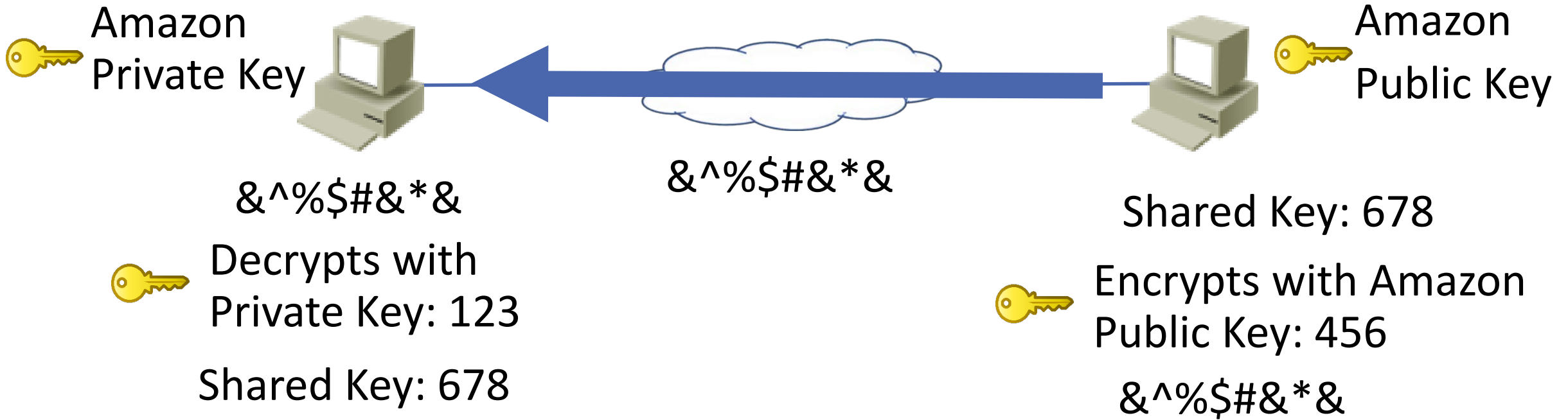
- The real Amazon.com is the only entity with their private key
- You have now authenticated Amazon.com

HTTPS Example

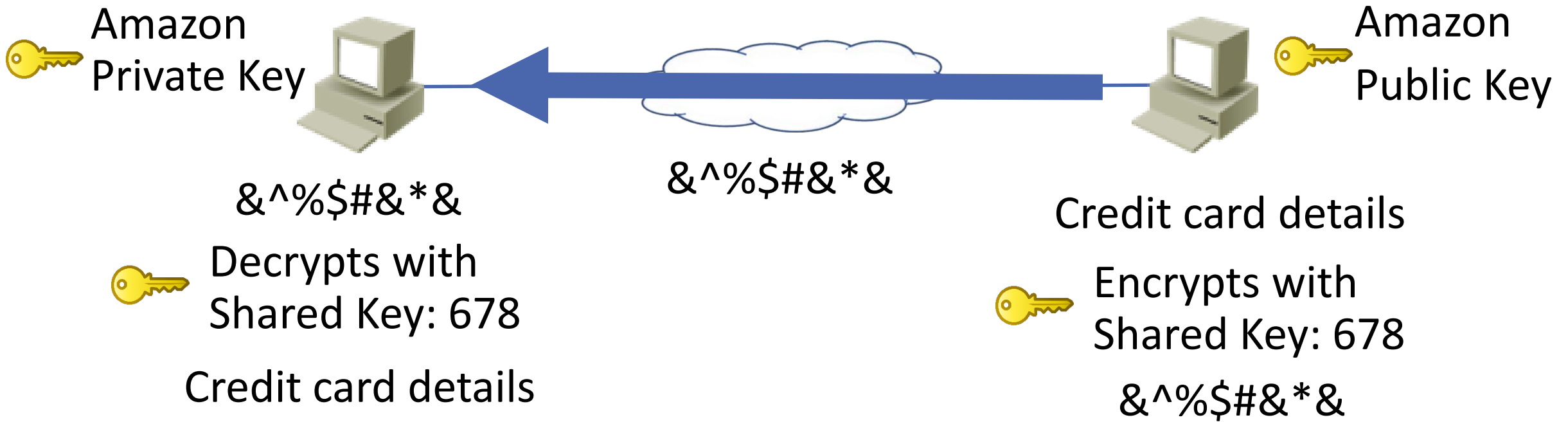


- Your browser could now encrypt your credit card details with Amazon's public key when you make a purchase, and nobody else would be able to read the details
- But asymmetric key encryption is slow and not suitable for bulk data exchange like web browsing
- Symmetric key encryption should be used, but Amazon and you do not have a shared key...

Asymmetric Encryption – Authenticity and Non-Repudiation



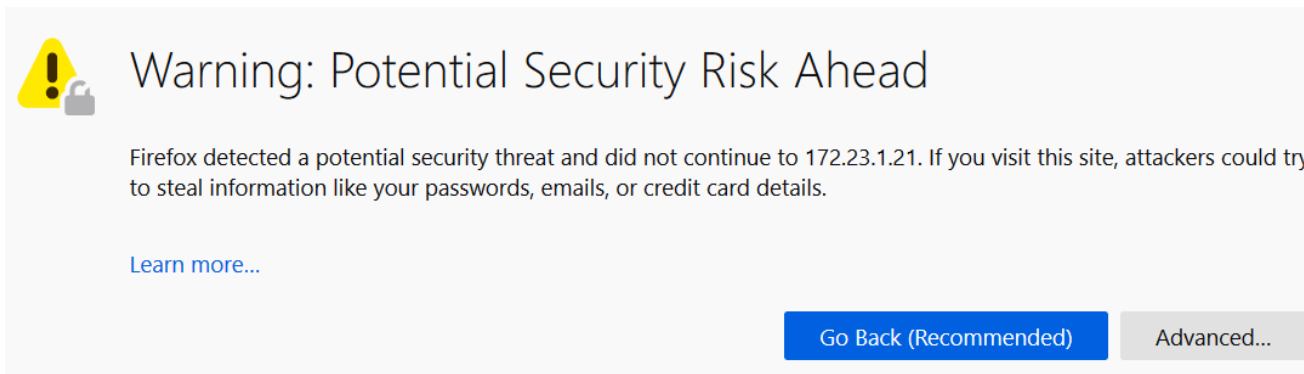
Asymmetric Encryption – Authenticity and Non-Repudiation




I Know What You're Thinking...



- Hackers also shop on Amazon and have a copy of Amazon's certificate. They could make a website looking like Amazon.com and trick you into going there (a phishing attack) then send you Amazon's certificate
- Your browser will ask them to authenticate with Amazon's private key and they don't have it



 Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 172.23.1.21. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

[Go Back \(Recommended\)](#) [Advanced...](#)

I Know What You're Thinking...




- A hacker could get a certificate for Amazon.com from a public Certificate Authority
- Public Certificate Authorities do out of band checks to verify they only issue legitimate certificates

I Know What You're Thinking...



- A hacker could open a business named 'Neil's Nuts' and get a public certificate for it, then trick you into going to a website that pretends to be Amazon.com and send you their Neil's Nuts certificate
- The certificate details which website it is valid for and is checked by your browser



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 172.23.1.21. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

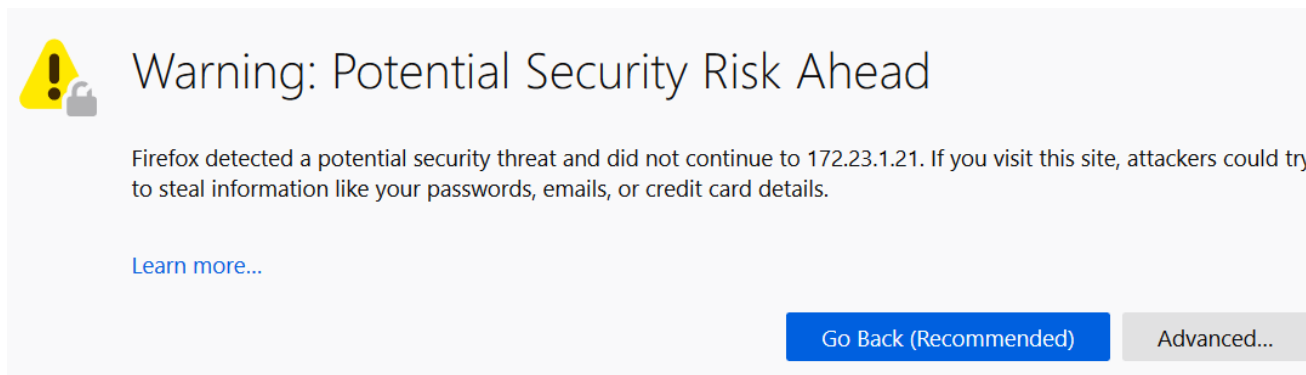
[Learn more...](#)


[Go Back \(Recommended\)](#) [Advanced...](#)

I Know What You're Thinking...



- A hacker could install their own certificate authority and create their own certificate for Amazon.com, then trick you into going to a website that pretends to be Amazon.com and send you their certificate
- Web browsers only trust certificates from trusted public Certificate Authorities



 Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 172.23.1.21. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

[Go Back \(Recommended\)](#) [Advanced...](#)

