

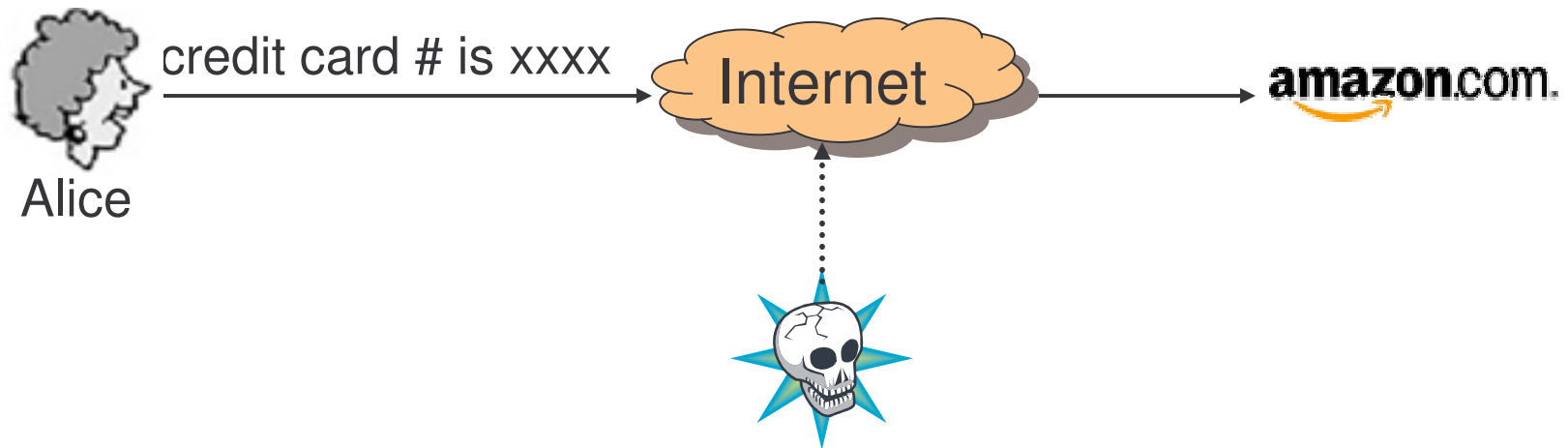
ECE 230x

Network Security Basics

Outline

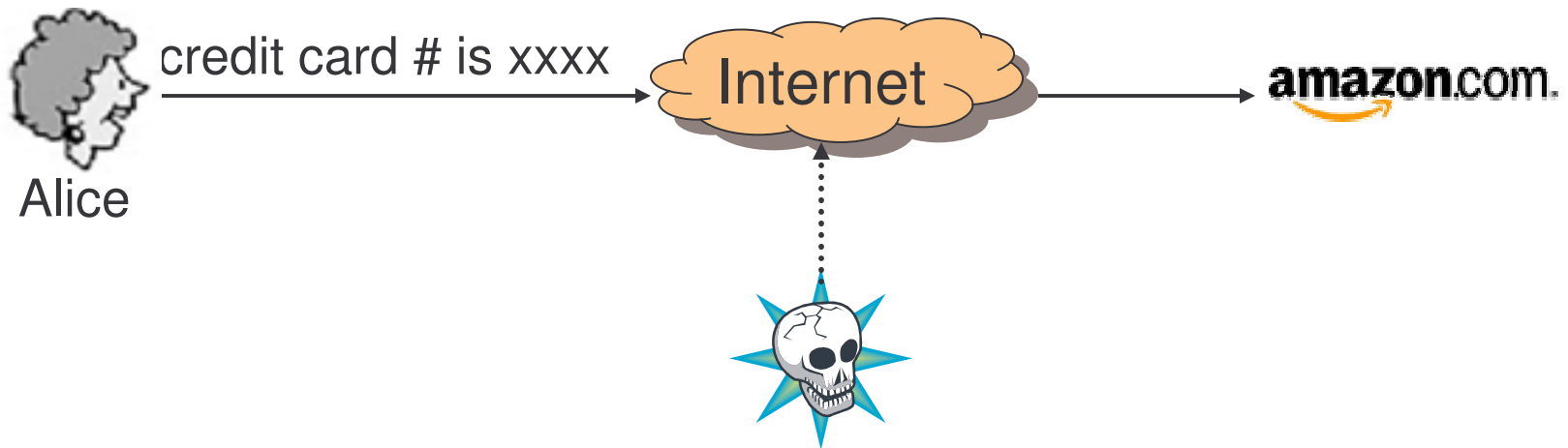
- Common security requirements
- Basic security tools
 - Secret-key cryptography
 - Public-key cryptography
- Example
 - Online shopping with Amazon

Common Security Requirements



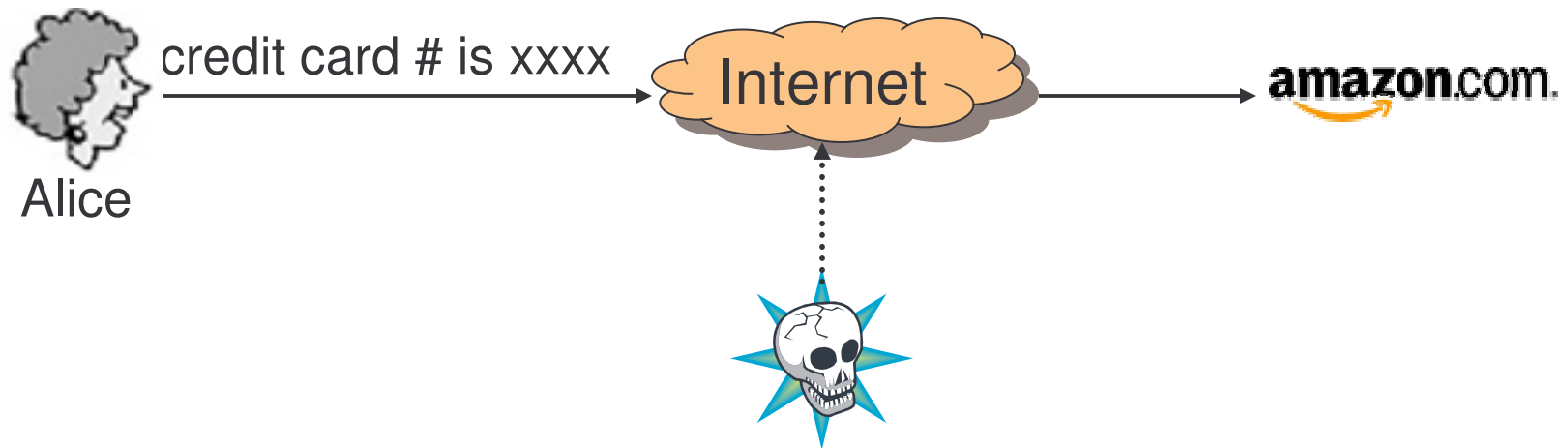
- What could the hacker possibly do?
 - Attempt to read the messages from Alice to Amazon, thus learning Alice's credit card number
 - Impersonate Amazon in the transaction – the *Phishing* attack
 - Modify the delivery address or content of Alice's order
- Do you still feel safe to do online shopping?
 - 85% of Americans have security concerns with online shopping, and 24% have abandoned it

Common Security Requirements



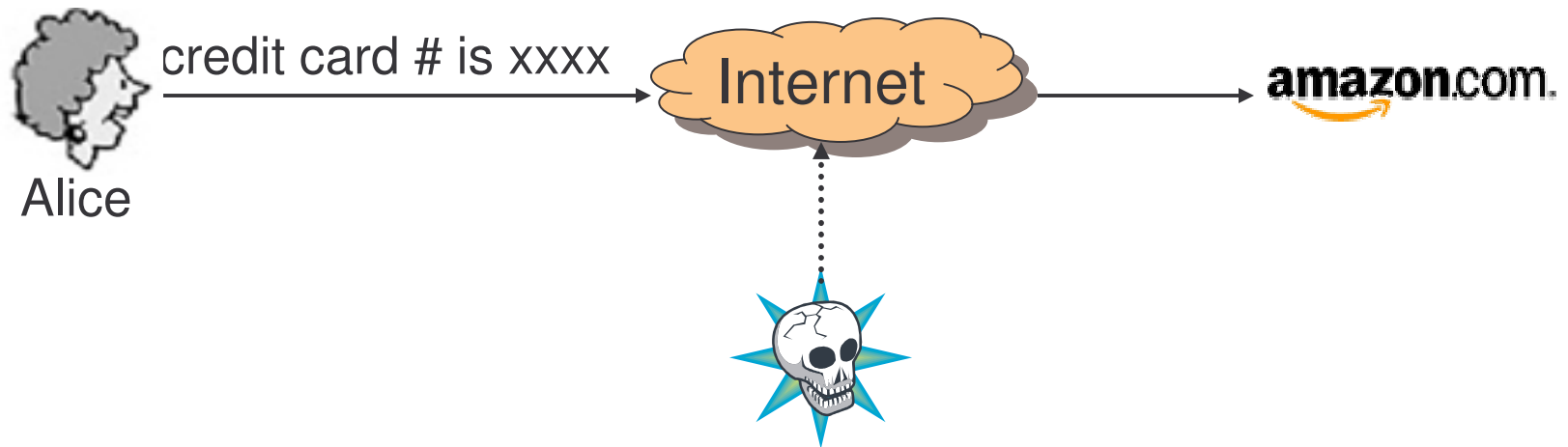
- Data confidentiality or secrecy
 - Message sent between Alice and Amazon should not be readable by or should appear unintelligible to the hacker
 - Preventing unauthorized access to secret data

Common Security Requirements



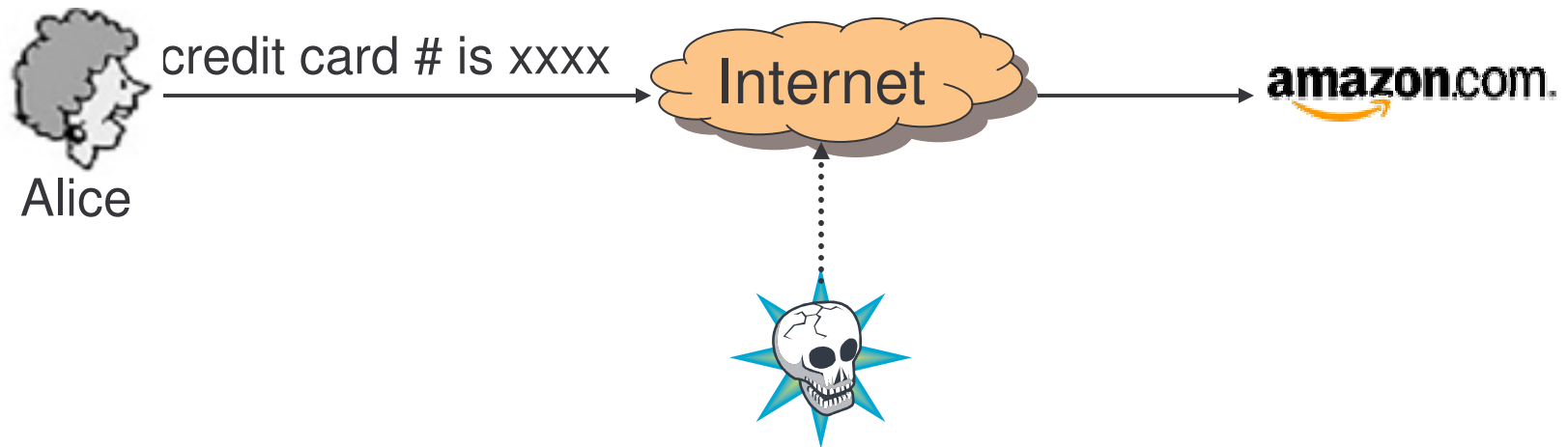
- Data integrity
 - Amazon should be able to detect if data sent by Alice has been modified by the hacker; vice versa
 - Ensuring data has not been altered by unauthorized means such as insertion, deletion, and substitution

Common Security Requirements



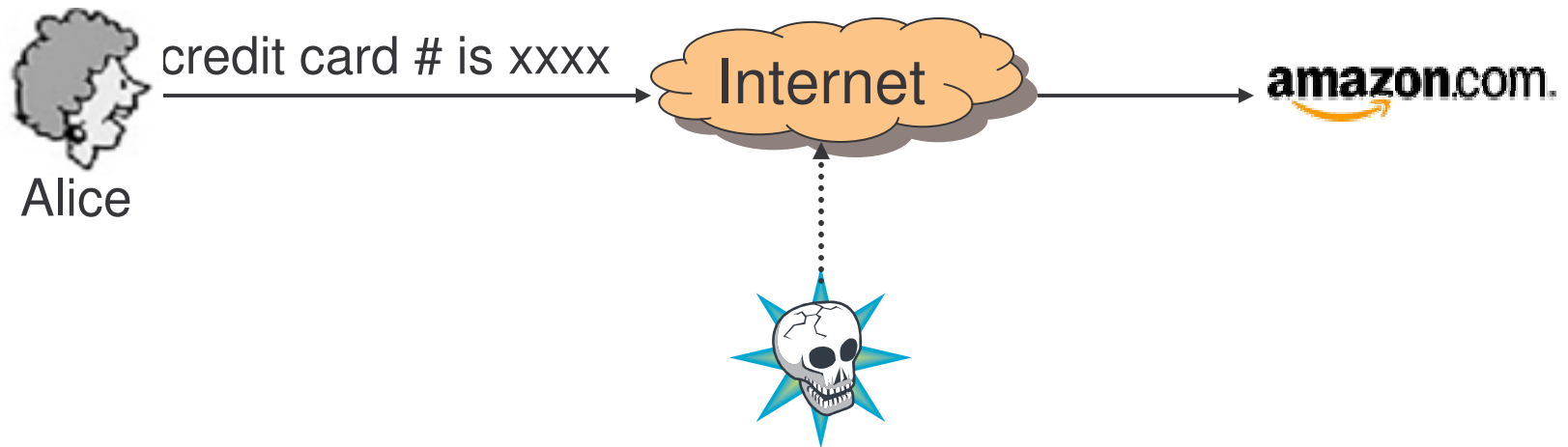
- Authentication
 - Alice and Amazon should be able to verify each other's identity
 - Enabling two communicating parties to identify each other

Common Security Requirements



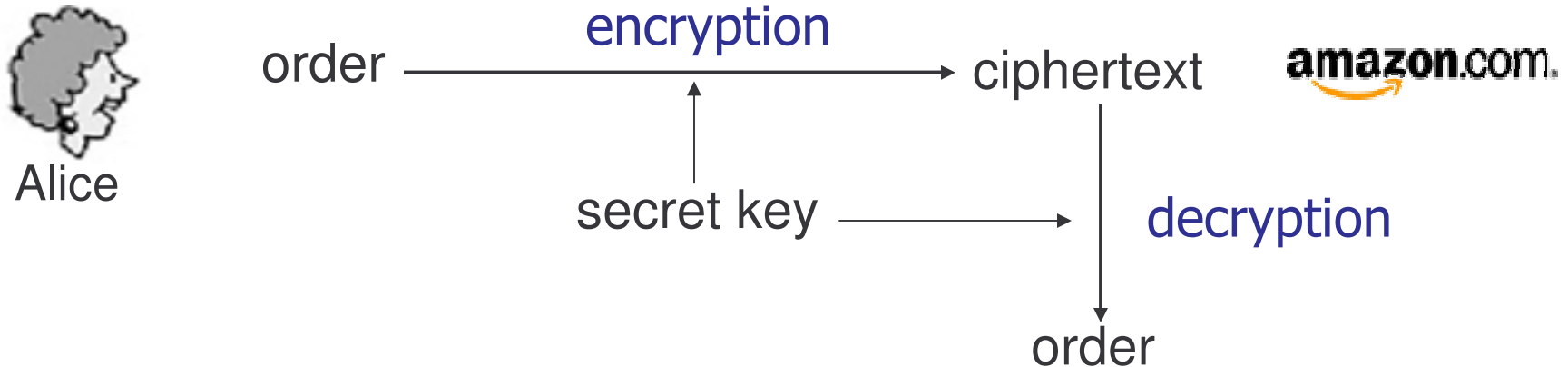
- Non-repudiation
 - Both Alice and Amazon cannot deny the transaction
 - Preventing an entity from denying previous commitments or actions

Secret-Key Cryptography



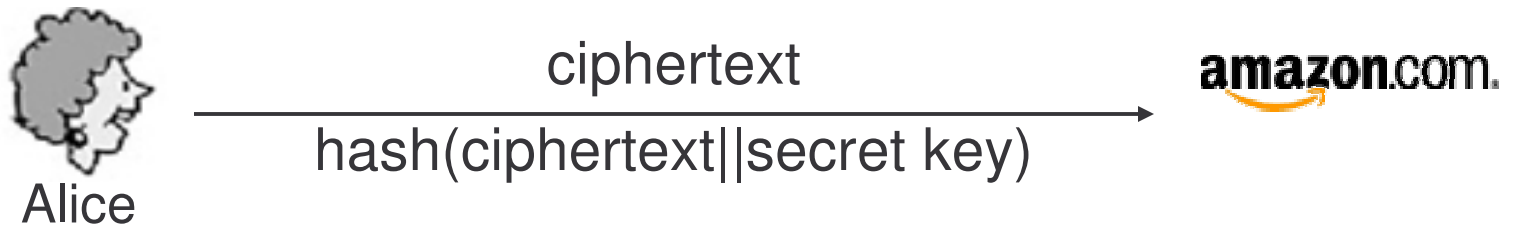
- Alice and Amazon share a common secret, which is called a secret key and only known to them two

Secret-Key Cryptography



- How is data confidentiality achieved?
 - Alice encrypts the order using the secret key and generates the ciphertext seeming unrelated to the original order
 - Amazon decrypts the ciphertext using the secret key
 - No one else can decrypt the ciphertext without the secret key

Secret-Key Cryptography



- Hash function
 - Taking an input message and produces a fixed-length output, called a *hash value*
 - It is infeasible to find two distinct input messages which hash to a common hash value
- How are data integrity and authentication achieved?
 - Alice sends to Amazon the ciphertext along with a hash value computed over the ciphertext and the secret key
 - Before doing decryption, Amazon recalculates the hash value and checks its equality to the received one
 - If the hash check is successful, Amazon determines the message was indeed sent by Alice and was not modified

Secret-Key Cryptography

- No support for non-repudiation
 - The secret key is known to two parties, e.g., both Alice and Amazon, and cannot be used to generate a unique digital signature
- Difficult secret-key establishment
 - How could Amazon establish a unique secret key with each of its millions of customers?

Public-Key Cryptography

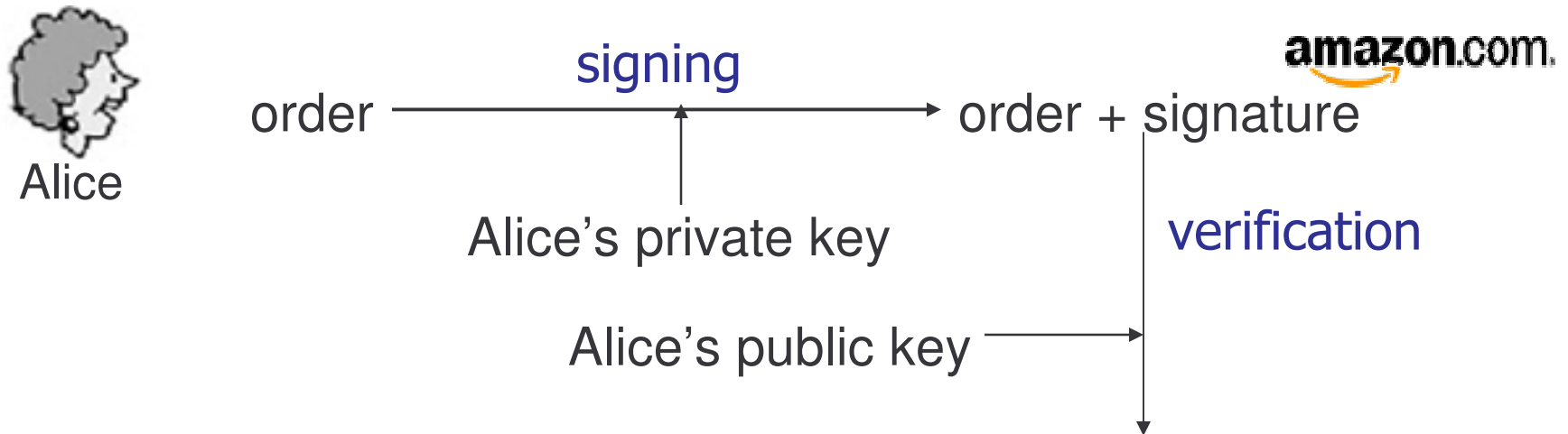
- Alice has two unique keys
 - A private key (K^{-1}), kept confidential to herself
 - A public key (K), preferably known to the entire world
 - There is a one-to-one correspondence between K & K^{-1}
 - It is computationally infeasible to determine K^{-1} given K
- Amazon also has unique pair of public and private keys

Public-Key Cryptography



- How is data confidentiality achieved?
 - Alice encrypts the order using Amazon's public key
 - Amazon decrypts the ciphertext using its private key
 - No one else can decrypt the ciphertext without knowing Amazon's private key

Public-Key Cryptography



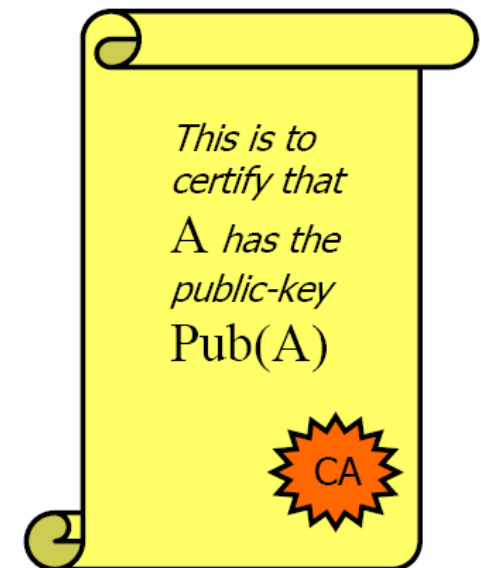
- Digital signatures provide guarantees for authentication, data integrity, and non-repudiation
 - Amazon trusts the order was sent by Alice and was not maliciously modified as nobody else can fake her digital signature
 - Alice cannot deny the order because only she knows her private key and can generate the signature on the order

Public-Key Cryptography

- How could Amazon know Alice's public key?
 - Alice sends her public key directly to Amazon
 - Or Alice puts her public key in some central public-key repository for Amazon to retrieve
- What is the security issue here?
 - The hacker modifies Alice's public key to his and thus is able to impersonate Alice to Amazon
 - The hacker modifies Amazon's public key to his and thus is able to impersonate Amazon to Alice
 - Called public-key impersonation attacks

Public-Key Cryptography

- Solution: public-key certificates
 - Signed messages specifying a name (Alice) and the corresponding public key
 - Generated by a trusted third party known as a Certification Authority (CA) whose public key is publicly known and trustable
 - For a list of common CAs, see http://dmoz.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities/
 - $\text{cert}_{\text{Alice}} := \langle \text{Alice}, K_{\text{Alice}}, \text{expiration-time}, \text{CA's signature} \rangle$
 - Amazon trusts K_{Alice} to be Alice's public key after verifying the CA's signature



Example: Online Shopping with Amazon



Ordering from Amazon.com is quick and easy

Enter your e-mail address:

- I am a new customer.**
(You'll create a password later)
- I am a returning customer,
and my password is:**

[Forgot your password? Click here](#)

[Has your e-mail address changed since your last order?](#)

The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our [standard server](#). You are buying this item from Amazon.com, Inc.

The only way to place an order at Amazon.com is via our Web site. (Sorry--no phone orders. However, if you prefer, you may phone in your credit card number, after filling out the order form online.)

Redeeming a gift certificate? We'll ask for your claim code when it's time to pay.

Having difficulties? Please visit our Help pages to learn more about placing an order.

[Conditions of Use](#) [Privacy Notice](#) © 1996-2006, Amazon.com, Inc.

Example: Online Shopping with Amazon

Amazon.com Checkout: Place Your Order - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://www.amazon.com/gp/flex/checkout/sign-in/select.html/002-9224611-0190467

Shipping Options: [\(Learn more\)](#)

Choose a shipping speed:

- Standard Shipping (3-5 business days)
- Two-Day Shipping (2 business days--get it Wednesday, April 12!)**
- One-Day Shipping (1 business day--get it Tuesday, April 11!)

The following items will arrive in 1 shipment:

Need to [Change quantities or delete](#)?

Estimated delivery date for this item: April 12, 2006 -- Wednesday

Network Security: Private Communication in a Public World, Second Edition - Charlie Kaufman
\$59.99 - Quantity: 1 - Usually ships in 24 hours - **Amazon Prime: Two-Day Shipping is free.**
Condition: new
Sold by: Amazon.com

Gift options None [Change](#)

Amazon Prime Shipping has been applied to the eligible items in your order.

Have any gift cards, gift certificates or promotional claim codes?
Enter them here (one at a time):
 [Apply](#)

Payment Method: [Change](#)
Amazon.com Visa:
***-82508
Exp: 01/2009

Billing Address: [Change](#)
Yanchao Zhang
329 University Vill
2
Gainesville, FL 32603
USA

Review the information above, then click "Place your order."

[Place your order](#)

If placing a Marketplace order you are also agreeing to the [Marketplace Participation Agreement](#)

Read Amazon.com's [pricing policy](#).

What happens when you place your order?

For an item sold by Amazon.com: When you click the "Place your order" button, we'll send you an e-mail message acknowledging receipt of your order. Your contract to purchase an item will not be complete until we send you an e-mail notifying you that the item has been shipped.

Amazon.com Returns Policy: Within 30 days of delivery, you may return new, unopened merchandise in its original condition. Exceptions and restrictions apply--read Amazon.com's complete [Returns Policy](#).

Example: Online Shopping with Amazon

The screenshot shows a Mozilla Firefox browser window titled "Amazon.com Checkout: Place Your Order". The address bar displays the URL: <https://www.amazon.com/gp/flex/checkout/sign-in/select.html/002-9224611-0190467>. The main content area is partially obscured by a "Page Info" dialog box. The dialog box has tabs for "General", "Forms", "Links", "Media", and "Security". The "Security" tab is active, showing the following information:

- Web Site Identity Verified:** The web site www.amazon.com supports authentication for the page you are viewing. The identity of this web site has been verified by Verisign, Inc., a certificate authority you trust for this purpose.
- View:** View the security certificate that verifies this web site's identity.
- Connection Encrypted: High-grade Encryption (RC4 128 bit)**
The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

In the background, the checkout page shows sections for "Choose a shipping speed:", "Payment Method:" (listing Amazon.com Visa), "Billing Address:" (listing chao Zhang, University Vill, nesville, FL 32603), and a "Place your order" button. A "Participation Agreement" link is also visible.

Example: Online Shopping with Amazon

- Major steps (SSL: Secure Sockets Layer Protocol)
 - Firefox initiates a session request to Amazon
 - Amazon returns its public-key certificate issued by VeriSign
 - Firefox uses the pre-stored VeriSign's public key to verify its signature in Amazon's public-key certificate
 - Firefox generates a secret key (a 48-byte number)
 - Firefox encrypts the secret key, and your web account and password with Amazon's public key, and sends the ciphertext to Amazon
 - Amazon uses its private key to decrypt the ciphertext and verifies your password
 - Subsequent communications between Firefox and Amazon will be encrypted and authenticated using secret-key techniques based on the shared secret key