Digital Money

COMP620

Blind Signatures

- A blind signature allows an authority to sign an object verifying its owner without revealing to the authority the content of the object
- The owner of the object should be able to get a signed copy of the object
  - Imagine putting a piece of paper in an envelope with carbon paper.
  - Someone can sign the envelope without reading the paper.
  - The owner can remove the paper with the signature

RSA Encryption

The RSA asymmetric encryption algorithm uses

- N = product of two large prime numbers
- d = secret exponent
- e = public exponent
- m = message
- x = encrypted message

$$x = m^d \pmod N$$

Blind RSA Signatures

- Assume a random number *r* that is relatively prime to N
- Let Y be a blinded version of m, the message

$$y = m * r^e \pmod N$$

- The blinded version can be signed

$$z = y^d \pmod N$$

- The owner can recover a signed message

$$x = z / r \pmod N$$

Explanation of Algorithm

- The random number has been raised to both the power of e and d
- e and d are inverses

$$r^{ed} = r \pmod{N}$$

- The message was originally multiplied by r
- Dividing by r restores the original message

Real Cash

- Real money is anonymous
- The Treasury department tries hard to make it difficult to copy money
- If destroyed, the value is lost

Digital Money Goals

- Consumers should not be able to generate their own money
- You should not be able to copy or reuse validly created digital money
- Attempts to defraud should identify the user
- Privacy should be maintained
- Simple failures should not lose money

Digital Money Idea 1

- Assume the First Digital Bank of Greensboro has an RSA key
- To withdraw a dollar from the bank, Alice generates a large random number and sends a digitally signed request for $X to the bank
- The bank verifies Alice's signature and saves the random number from the requesting message

Digital Money Idea 1 (continued)

- The bank withdraws $X from Alice's account
- A digitally signed note for $X is sent to Alice
- To buy something at Bob's store, Alice gives him the note she received from the bank
- Bob checks the digital signature to verify it comes from First Digital Bank
- Bob transmits the note to the bank

Digital Money Idea 1 (continued)

- The bank verifies its signature and checks the random number to ensure it has not been previously spent
- The bank deposits $X into Bob's account
- A digitally signed deposit slip is sent to Bob
- Bob can give Alice a digitally signed receipt and the goods she purchased

Security but not Privacy

- All transactions are signed, so none of entities involved can deny the action
- The transactions could have been encrypted with the receivers public key to provide confidentiality
- The bank could keep track of where Alice is spending her money
- The bank can also keep track of Bob's customers

eCash

- David Chaum developed blind signatures and processes for handling digital money
- Each bank has a set of digital certificates, one for each denomination of digital money

Digital Money Idea 2

- Alice agrees to purchase a widget from Bob for $X
- Bob sends a request to his bank for a $X deposit slip. The request includes a random number
- Bob's bank saves the random number and digitally signs Bob's deposit slip
- The digitally signed deposit slip is sent to Bob

Digital Money Idea 2 (continued)

- Bob sends the digitally signed deposit slip to Alice
- Alice blinds the deposit slip with her digital certificate
- She sends the blinded deposit slip to her bank with a request to withdraw $X
- The bank withdraws $X from Alice's account
- The blinded deposit slip is signed by Alice's bank using their $X digital certificate

Digital Money Idea 2 (continued)

- Alice's bank sends her the digitally signed blinded deposit slip
- Alice unblinds the deposit slip. It is still digitally signed by her bank using their $X certificate
- Alice sends the deposit slip to Bob
- Bob sends the deposit slip to his bank

Digital Money Idea 2 (continued)

- Bob's bank verifies the signature of Alice's bank for $X
- Bob's bank also checks its digital signature
- The random number in the deposit slip is checked to make sure it was given to Bob
- If all checks pass, Bob's account is credited with $X
- Bob is sent a signed statement that $X was deposited

Secure and Anonymous

- Bob's bank knows that funds were withdrawn from Alice's bank, but does not know from which account
- Alice's bank knows she made a withdraw, but does not know to whom the deposit was made

Issues

- It may be difficult for the government to monitor the flow of money
  - Money laundering
  - Quantity of available money