Last Time....
Secret-Key Encryption

\[ m_0 \oplus \text{Enc}(sk) \rightarrow c_0 \]
\[ m_1 \oplus \text{Enc}(sk) \rightarrow c_1 \]
\[ m_2 \oplus \text{Enc}(sk) \rightarrow c_2 \]
\[ m_3 \oplus \text{Enc}(sk) \rightarrow c_3 \]
\[ m_4 \oplus \text{Enc}(sk) \rightarrow c_4 \]
Number Theory

computing $g^x \mod p$ is easy
computing $\log_g y \mod p$ is hard
Diffie-Hellman Key Exchange

Alice

Bob

\[ y_A = g^{x_A} \]

\[ y_B = g^{x_B} \]

\[ y_B^{x_A} = g^{x_A x_B} \]

\[ y_A^{x_B} = g^{x_A x_B} \]
Public-Key Encryption

\[ c = \text{Enc}_{pk}(m) \]

\[ m = \text{Dec}_{sk}(c) \]
Hybrid Encryption

generate a session key \( session\_key \)

\[ c = Enc_{session\_key}(m), Enc_{pk}(session\_key) \]
Signatures

\[ \text{Sign}_{sk}(m) = \sigma \]

\[ \text{Verify}_{pk}(m, \sigma) = \text{True/False} \]

Reverse the Public-Key Encryption operation!

\[ \text{Sign}_{sk}(m) = \text{Dec}_{sk}(m) \]

\[ \text{Verify}_{pk}(m, \sigma) \rightarrow \text{Enc}_{pk}(\sigma) \overset{?}{=} m \]
Hash Functions

\[ H(m) = \text{hash}, \text{Sign}_{sk}(H(m)) \]

- “fingerprint” of a long document
- MD5 hashes to 128 bits, SHA1 hashes to 160 bits
- Properties
  - Collision Attack
  - Pre-Image Attack
  - Second Pre-Image Attack
Certificates

\[ cert = \text{Sign}_{TTP}( \text{"Bob, pk}_B \text{"}) \]

Alice \quad \quad \text{pk}_B, cert \quad \quad \text{Enc}_{\text{pk}_B}(m) \quad \quad \text{Bob}

TTP
PGP

Alice

Bob

Charlie

Sign_{Charlie}(“Bob”, pk_{Bob})

pk_{Charlie}

pk_{Bob}

Enc_{pk_{Bob}}(message)
Advanced Applications
Anti-Phishing
I HAVE A NEW HOBBY. IT'S CALLED PHISHING.

I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.

Dear Customer,
This is your bank. We forgot your social security number and password. Why don’t you send them to us so we can protect your money.

Sincerely,
I. B. Banker
From: eBay Billing Department <Billing@eBay.com>
Subject: Credit/Debit Update
Date: April 8, 2005 6:48:27 PM EDT
To: Ben Adida (E-mail)

Dear eBay member,

We at eBay are sorry to inform you that we are having problems with the billing information of your account. We would appreciate it if you would visit our eBay Billing Center and fill out the proper information that we are needing to keep you as an eBay member. If you don't comply until the 15 April 2005, your eBay membership may be suspended, or even deleted.

Click here to complete our web form.

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Thank you!
My eBay

New to eBay?  or  Already an eBay user?

If you want to sign in, you'll need to register first.
Registration is fast and free.

View all your bidding and selling activities in one location.

**eBay User ID**

Forgot your User ID?

**Password**

Forgot your password?

Sign In Securely >

Keep me signed in on this computer unless I sign out.

Account protection tips
Be sure the Web site address you see above starts with https://signin.ebay.com/

Microsoft Passport users click here.
One in 20 'fall for online fraud'

One in 20 UK internet users say they have lost money through online scams, research into spam emails suggests.

Almost half say they have received so-called phishing emails aimed at tricking them into revealing details like online banking passwords.
this review is gathering information from community members on their usage of and satisfaction with medical care at MIT, and the Task Force has constructed a survey for students to provide their feedback.

Your time is valuable, especially at this busy time of year, but I hope that you might be willing to take about fifteen minutes to complete a web-based questionnaire. Your participation is entirely voluntary, and you may answer as few or as many questions as you wish. Your response will be treated as confidential, and data gathered will be reported in summary format. I urge you to be as candid as possible in your answers, as this is a very important issue for you and for the students who will follow you at MIT.

You may enter the survey from <http://web.mit.edu/surveys/medical/>. This survey authentication requires a current MIT certificate.

If you have any questions, please send them to med-survey@mit.edu.

Sincerely,
Susan Hockfield
Beware: E-Mailed Surveys May Involve 'Phishing'
Scammers Seek Bank Account Numbers
By Audrey Laganas
From: Burgess-Gregg, Mary  
Sent: Thursday, December 02,  
Subject: Presidential Recognition  

I am pleased to inform you that more specific at this point be candidates.

I am contacting you now because we need to request a name check from the FBI, as we do with all persons being considered for Presidential recognition. In light of procedures put in place by the White House Counsel's Office, we must receive your written consent prior to requesting the name check. The request a name check from the FBI,  

http://ostp.gov/FBInamecheck.pdf

form should be faxed immediately,  

NEOB  
(202) 456-6130  
(202) 456-6027 (fax)  
MBurgess-Gregg@ostp.eop.gov
Fax Attack

New scam asks people to fax away data
Published: August 11, 2005, 7:48 AM PDT

By Dawn Kawamoto
Staff Writer, CNET News.com

Phishers have added a new lure to their tackle boxes: e-mails that ask people to fax sensitive information to bogus security investigators.
Phishers try a phone hook

By Joris Evers
Staff Writer, CNET News.com
Published: April 27, 2006, 5:51 PM PDT

In a new twist on phishing, fraudsters are sending out e-mails that attempt to trick people into sharing personal information over the phone.
SMTP Today

Alice

DNS

foo.com
MX Record
mail.foo.com

wonderland.com
outgoing mail server

MX

mail.foo.com
incoming mail server

Bob

1

SMTP Today

2

3

4
No Proof of Origin
# A Platform of Trust

We want to provide Just Enough Trust

<table>
<thead>
<tr>
<th>User Interface Indicators</th>
<th>Reputation Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Light Sigs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Automatic Filtering</th>
<th>Reputation Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Light Sigs</td>
</tr>
</tbody>
</table>
Basic Signatures

\[
\text{sign}_{\text{wonderland}}(PK_{alice}, \text{"alice@wonderland.com"})
\]
DNS to distribute Domain-Level Keys

[DomainKeys]
Email Authentication

From: Alice
to: Bob
Subject: 6.976
It's the best class I've ever taken, seriously. You should take it.

Alice
Email Authentication

- certifying a user’s public key can add significant overhead.
- distributing the secret key to all user access points is tricky.

... unless we rethink the security requirements a bit.
Email-Based Authentication

[Gar2003]
Server-Managed User Keys

**Authority**
- wonderland
- $SK_{wonderland}$
- $PK_{wonderland}$

**DNS**
- wonderland.com
- $PK_{wonderland}$

**Incoming mail server**
- wonderland.com

**From:** Alice
**To:** Bob
**Subject:** 6.976

It's the best class I've ever taken, seriously. You should take it.

Alice

$$sign_{alice}(message)$$
$$PK_{alice}$$
$$sign_{wonderland}(PK_{alice}, "alice@wonderland.com")$$

**Bob**
bob@foo.com
DomainKeys

Authority

wonderland

SK\textsubscript{wonderland}

DNS

wonderland.com

PK\textsubscript{wonderland}

From: Alice
To: Bob
Subject: 6.976
It's the best class I've ever taken, seriously. You should take it.

Alice

From: Alice
To: Bob
Subject: 6.976
It's the best class I've ever taken, seriously. You should take it.

Alice

Bob

bob@foo.com
Can we get the benefits of both user keys and domain keys?
ID-Based Crypto

Keyserver

Alice

Bob

"bob@foo.com"

PK_{bob}

SK_{bob}

MPK

MSK

P K_{bob}

S K_{bob}
ID-based Domains

Alice

Bob
DNS to distribute Master Public Keys

DNS

wonderland.com

$MPK_{\text{wonderland.com}}$

foo.com

$MPK_{\text{foo.com}}$

Publish

wonderland.com

key server

$MSK_{\text{wonderland.com}}$
Email-Based Authentication for User Secret Keys

Alice

wonderland.com
incoming mail server

wonderland.com
keyserver

MSK_{wonderland.com}

SK_{alice@wonderland.com}

Alice
Lightweight Signatures

1. **PUBLISH**

   - **wonderland.com**
   - **key server**

2. **$SK_A$**

3. **Alice**
   - **Wonderland.com Network**

4. **From:** Alice
   - **To:** Bob
   - **Subject:** 6.976!
   - **Signed:** Alice
   - Dev is the best professor ever!

5. **MPK_{bank}**

6. **Bob**
   - **foo.com Network**
So What?

- Alice likes Bob
- Eve likes Bob
- Bob likes to gloat.

What if Bob publishes Alice’s Email on his blog?

This changes the nature of email.
Hey Bob,

Wanna meet for coffee? I'd love to get to know you better.

Signed: 
Alice or Bob
A Taste of Voting
Voting is Hard

Verifiability

Anonymity
The Point of An Election

“The People have spoken.... the bastards!”

Dick Tuck
1966 Concession Speech

Provide enough evidence to convince the loser.
Ben: “Bob”

Ron: “Bob”

Whit: “Bob”

Franz: “Alice”

Kevin: “Alice”
Can we get ballot secrecy and election audit-ability?
Encrypted Bulletin Board

Kevin: x38vf
Franz: e3s823
Ron: dfuciv2
Ben: d9cv0
Whit: n7390n
Verification?

Ballot Casting Assurance

Vote: Alice
Kevin

Universal Verifiability

Tally: Bob

Ben: d9cv0
Franz: e3s823
Whit: n7390n
Ron: dfuciv2
Kevin: x38vf
Zero-Knowledge Proofs
“How to Explain Zero-Knowledge to Your Children”

Quisquater & Guillou

graphics from Wikipedia
“How to Explain Zero-Knowledge to Your Children”

Quisquater & Guillou

graphics from Wikipedia
Envelopes

Favorite: Alice

This last envelope probably contains “Alice”
Graph 3-Coloring
Graph 3-Coloring
Graph 3-Coloring
Graph 3-Coloring
What did you learn?

Nothing more than the fact that I probably know a true 3-coloring.
In particular

You did not learn enough to prove this same property to someone else.

Smells like....
Proving the content of a vote while preventing vote selling!
Alice Voter Registration Database

Bob Voter

Carol Voter

Anonymousization

Decryption

Encrypted Votes

Encryption

Registration Database

Results
Each mix server shuffles and rerandomizes the ciphertexts in private.
Decryption Mixnet

\[ c = \text{Enc}_{pk_0}(\text{Enc}_{pk_1}(\text{Enc}_{pk_2}(m))) \]

Each mix server “unwraps” a layer of this encryption onion.
Verifying a Dec. Mixnet

1/2 of mix servers honest = no complete path is revealed

Randomized Partial Checking - Juels, Jakobsson, Rivest 2002
Prêt-à-Voter

H(Onion) that routes the ballot through a Chaumian mixnet to recover the candidate order.
Questions?