CSE 484 / CSE M 584 (Winter 2009)

Cryptography (Introduction)

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Goals for Today

- Cryptography Background
- Start, if time: Symmetric (Shared-Key Foundations)

- Reminder: Make progress on the lab
- Reminder: Homework 1 due on Friday

Security in the News

IT: Storm Worm Botne

Posted by timothy on Sunday Janu
from the **after-honeynets-let's-try-b**

Heise Security reports that a 'team
University and RWTH Aachen Uni
notorious Storm Worm botnet, and
isn't as invulnerable as it once see
for in theory it can be rapidly elimin
developed and at least partially dis
Tillmann Werner, Felix Leder and
in practice the elimination process

Read More | 217 comments

Your Rights Online: Mumbai Police To Enforce Wi-Fi Security

Posted by Soulskill on Saturday January 10, @01:22PM
from the **taking-a-stand-against-e-loitering** dept.

caffeinemessiah writes

> "In the wake of the recent terrorist attacks in Mumbai, India, the local police are going to be sniffing out unsecured wi-fi access points and ordering the owners to secure them. The article notes that 'terror mails were sent through unsecured Wi-Fi connections' before bomb blasts in other Indian cities. No word on if they'll be walking around using Kismet, or if people who use pathetically weak WEP encryption will be ordered to switch to more advanced protocols. Unfortunately, a gesture like this does not take into account the insidious scenario of walking into a cafe, buying a coffee and then (legally) using the cafe's wi-fi. Or the fact that terrorists might actually be able to pay to use a cybercafe, and know what VPNs are."

On the other hand, the Mumbai police may still be keeping track of the mandatory keyloggers that went into the area's cybercafes in 2007.

government networking security bigbrother

Read More | 129 comments yro privacy story

Your Rights Online: **ASCII Art Steganography**

Posted by timothy on Monday January 12, @03:37AM
from the **of-all-the-ideas-out-there-this-is-one** dept.

bigearcow writes

> "ASCII art is nothing new, but this site takes it one step further by allowing you to embed another data file within the image. The resulting ASCII art remains printable (i.e. no special unicode symbols) — this means you can print the image out, hang it on your wall, and have it look like an innocent ASCII art when it's hiding a secret document of your choice."

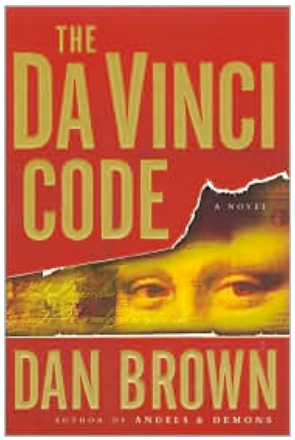
You'll need a small (200x200 pixel max) base image from which the ASCII art will be built.

▶ security graphics encryption slashdotted yro privacy story

Read More | 99 comments

Cryptography and Security

- Art and science of *protecting* our *information*.
  - Keeping it private, if we want privacy
  - Protecting its integrity, if we want to avoid forgeries.



Images from Wikipedia and Barnes and Noble

Some thoughts about cryptography

- Cryptography only one small piece of a larger system
- Must protect entire system
  - Physical security
  - Operating system security
  - Network security
  - Users
  - **Cryptography** (following slides)
- Security only as strong as the weakest link
  - Need to secure weak links
  - But not always clear what the weakest link is (different adversaries and resources, different adversarial goals)
- Cryptography helps after you've identified your threat model and goals

boingboing
A Directory Of Wonderful Things

sed risk

Biometric car lock defeated by cutting off owner's finger

POSTED BY CORY DOCTOROW, MARCH 31, 2005 7:53 AM | PERMALINK

Andrei sez, "'Malaysia car thieves steal finger.' This is what security visionaries Bruce Schneier and Ross Anderson have been warning about for a long time. Protect your $75,000 Mercedes with biometrics and you risk losing whatever body part is required by the biometric mechanism."

> ...[H]aving stripped the car, the thieves became frustrated when they wanted to restart it. They found they again could not bypass the immobiliser, which needs the owner's fingerprint to disarm it.
>
> They stripped Mr Kumaran naked and left him by the side of the road - but not before cutting off the end of his index finger with a machete.

Key Entry Pad (4-digit PIN)

Image from profmason.com

- This is the key pad on my office safe.
- Inside my safe is a copy of tomorrow's final exam.
- How long would it take a you to break in?

- Answer (combinatorics):
  - 10^4 tries *maximum*.
  - 10^4 / 2 tries on *average*.
- Answer (unit conversion):
  - 3 seconds per try --> 4 hours and 10 minutes on average

Key Entry Pad (4-digit PIN)

Image from profmason.com

- Now assume the safe automatically calls police after 3 failed attempts.
- What is the probability that you will guess the PIN within 3 tries?
- (Assume no repeat tries.)

- Answer (combinatorics):
  - 10000 choose 3 possible choices for the 3 guesses
  - $1 \times (9999 \text{ choose } 2)$ possible choices contain the correct PIN
  - So success probability is 3 / 10000

Key Entry Pad (4-digit PIN)

- Could you do better at guessing the PIN?

- Answer (*chemical* combinatorics):
  - Put different chemical on each key (NaCl, KCl, LiCl, ...)

Image from profmason.com

Idea from http://eprint.iacr.org/2003/217.ps

Key Entry Pad (4-digit PIN)

- Couldyou do better at guessing the PIN?

- Answer (*chemical* combinatorics):
  - Put different chemical on each key (NaCl, KCl, LiCl, ...)
  - Observe residual patterns after 1 access safe

Image from profmason.com

Idea from http://eprint.iacr.org/2003/217.ps

Key Entry Pad (4-digit PIN)

- Could you do better at guessing the PIN?

- Answer (*chemical* combinatorics):
  - Put different chemical on each key (NaCl, KCl, LiCl, ...)
  - Observe residual patterns after 1 access safe

Image from profmason.com

Idea from http://eprint.iacr.org/2003/217.ps

Key Entry Pad (4-digit PIN)

- Could you do better at guessing the PIN?

- Answer (*chemical* combinatorics):
  - Put different chemical on each key (NaCl, KCl, LiCl, ...)
  - Observe residual patterns after I access safe

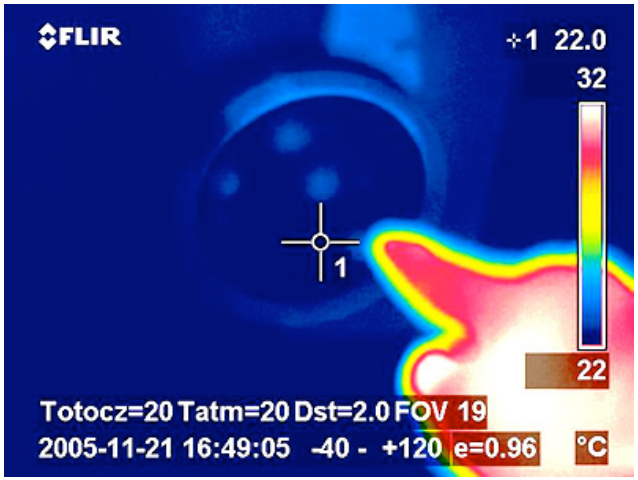
Lesson: Consider the complete system, physical security, etc

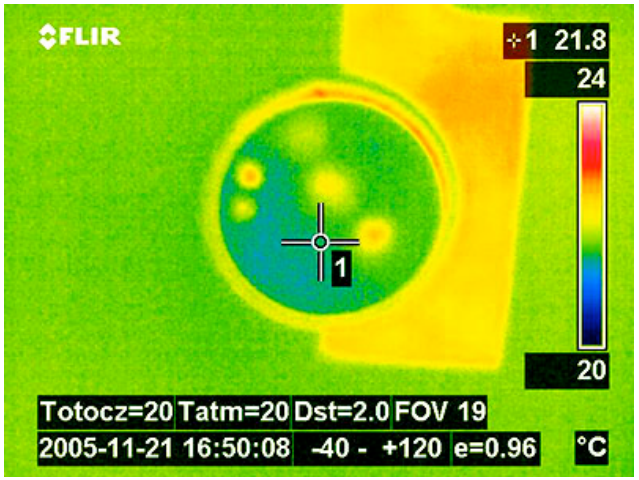
Lesson: Think outside the box

Image from profmason.com

Idea from http://eprint.iacr.org/2003/217.ps

Thermal Patterns



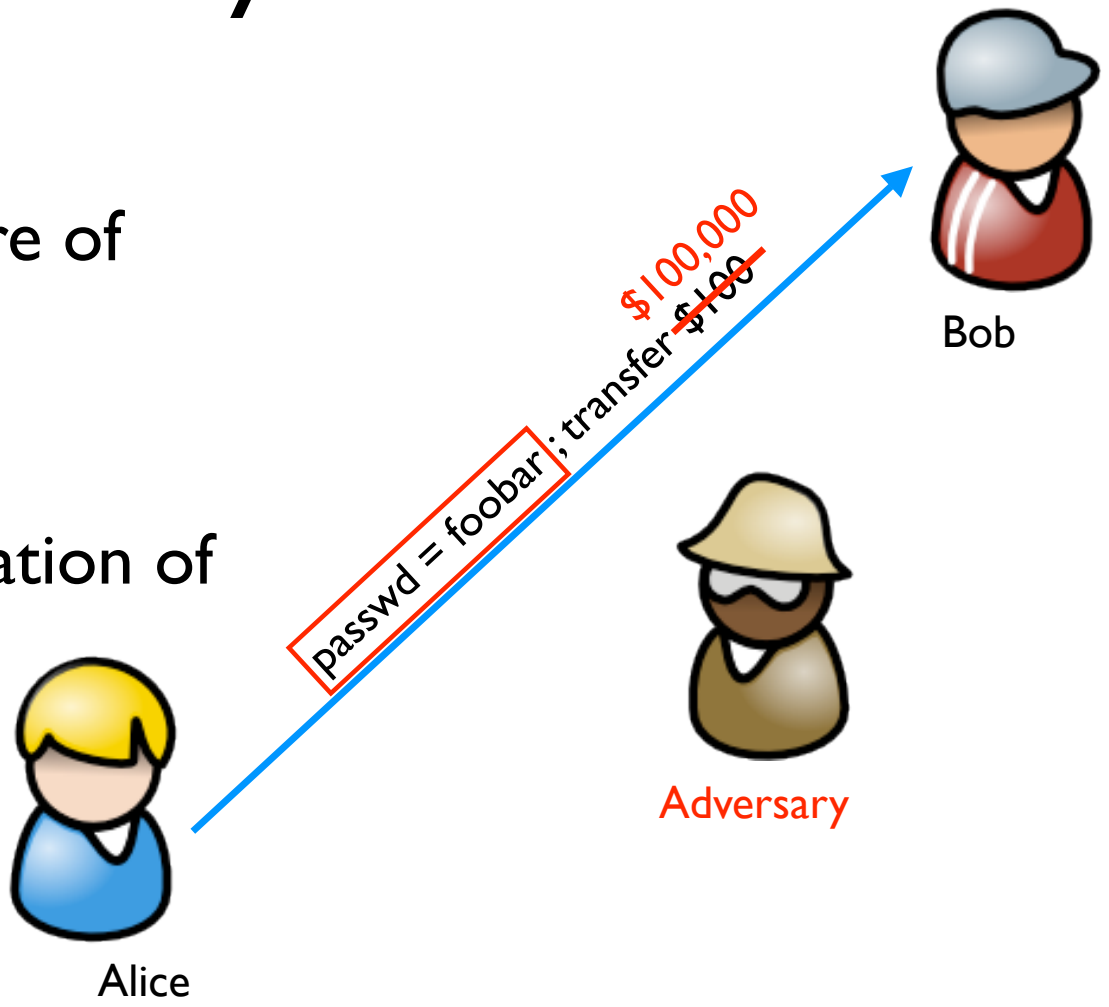


Images from http://lcamtuf.coredump.cx/tsafe/

Common Communication Security Goals

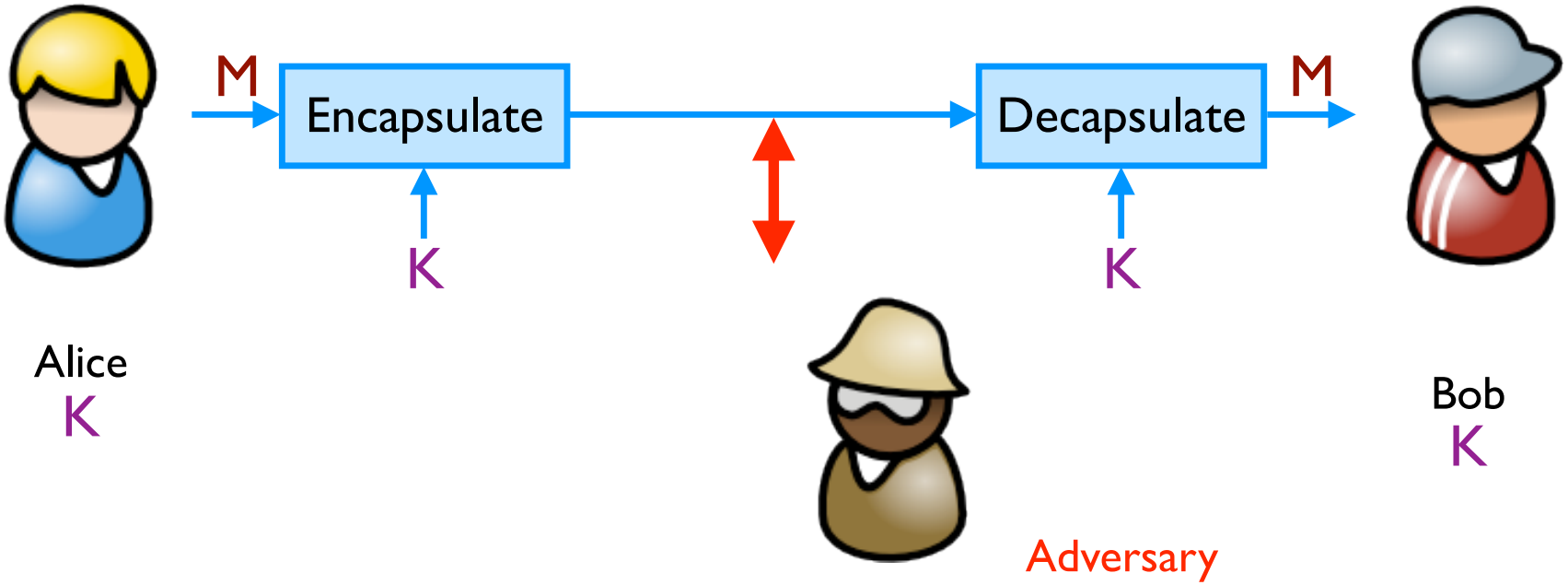
Privacy of data
Prevent exposure of information

Integrity of data
Prevent modification of information



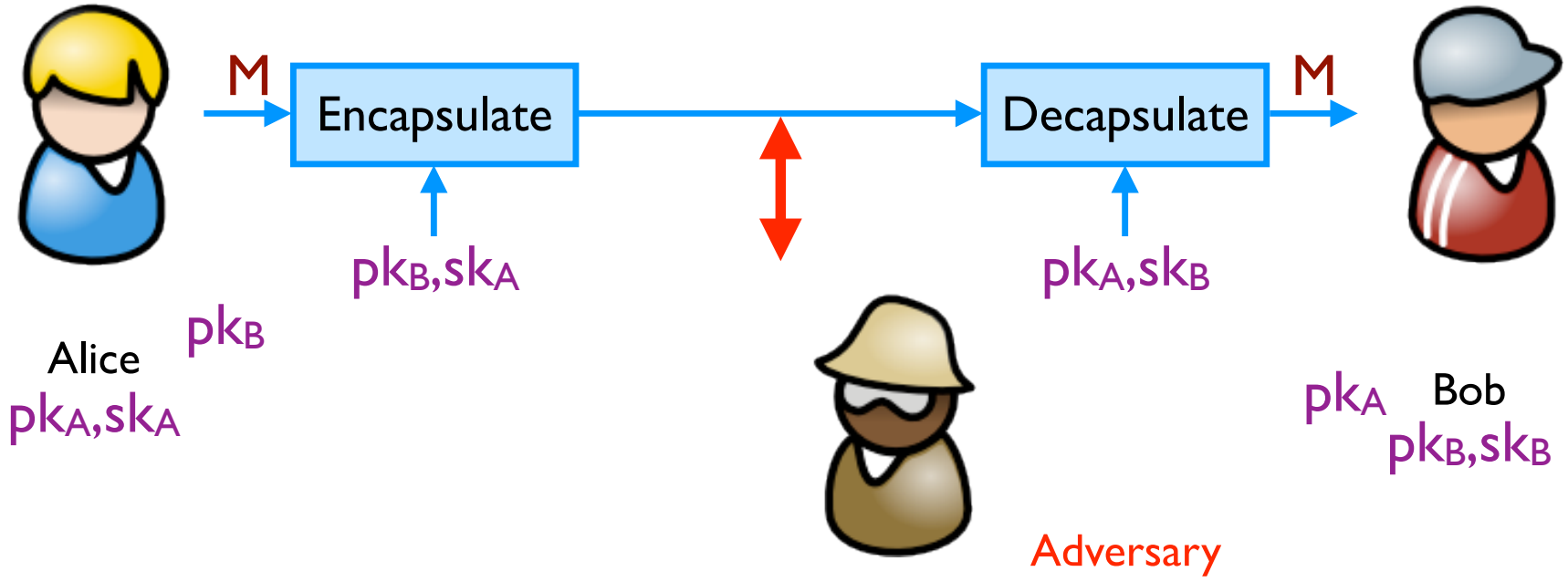
Symmetric Setting

Both communicating parties have access to a shared random string K, called the key.



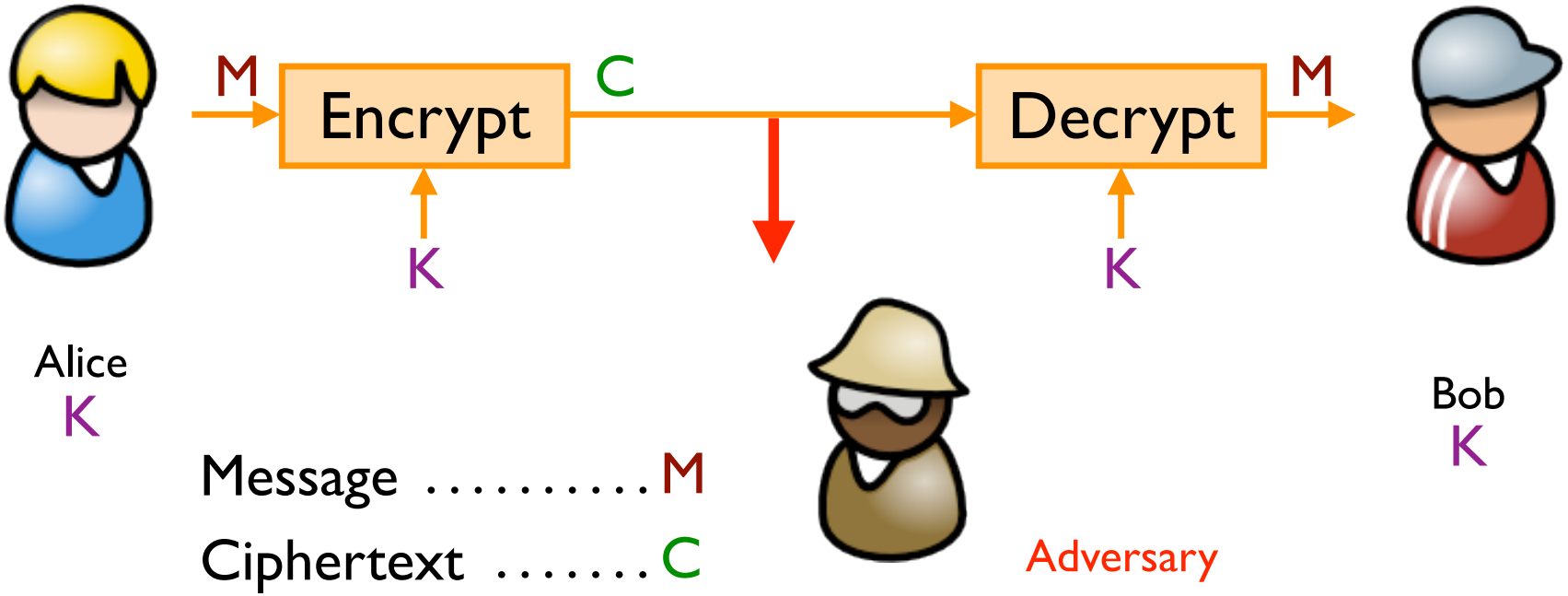
Asymmetric Setting

Each party creates a public key pk and a secret key sk.



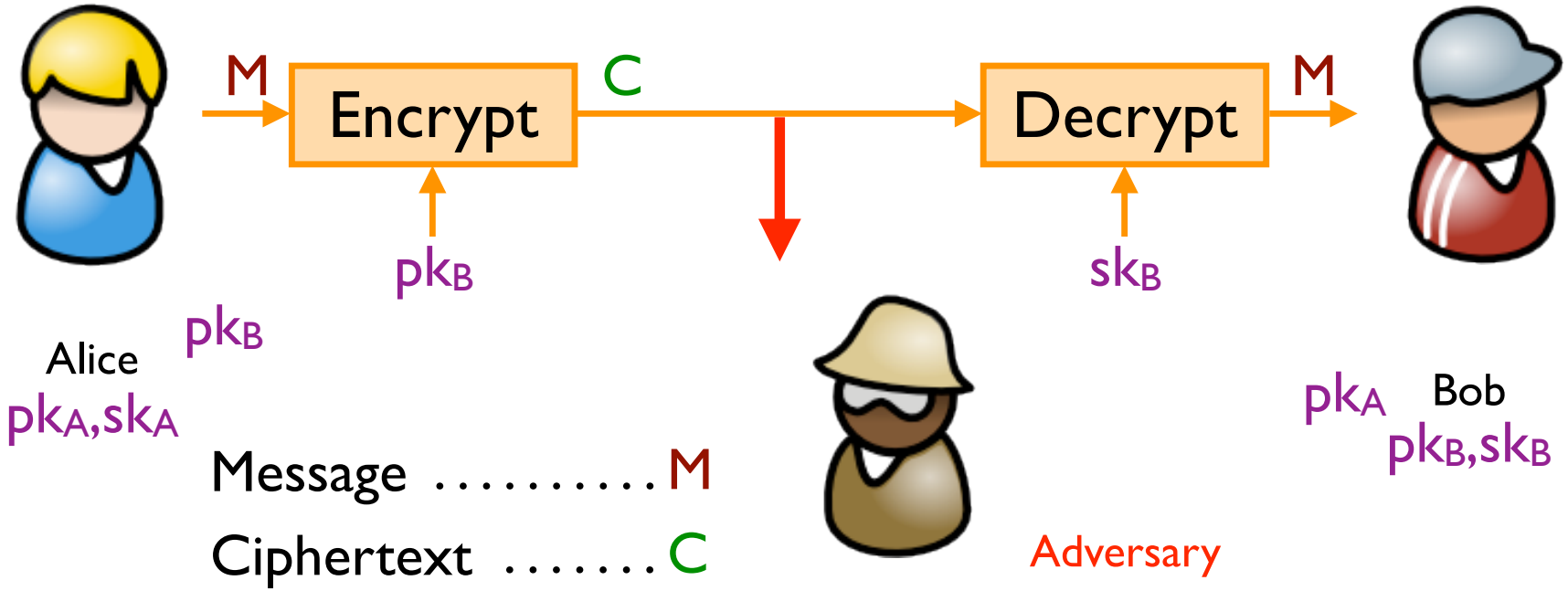
Achieving Privacy (Symmetric)

Encryption schemes: A tool for protecting privacy.



Achieving Privacy (Asymmetric)

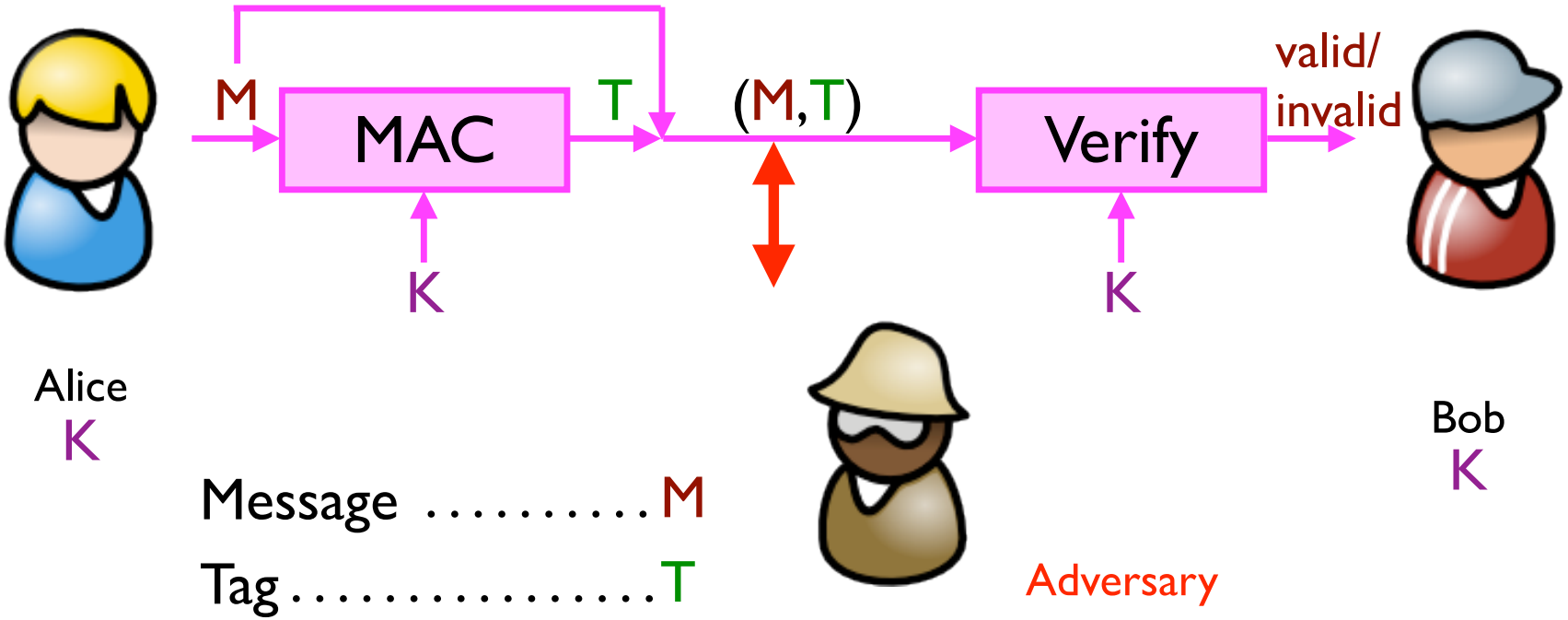
Encryption schemes: A tool for protecting privacy.



Achieving Integrity (Symmetric)

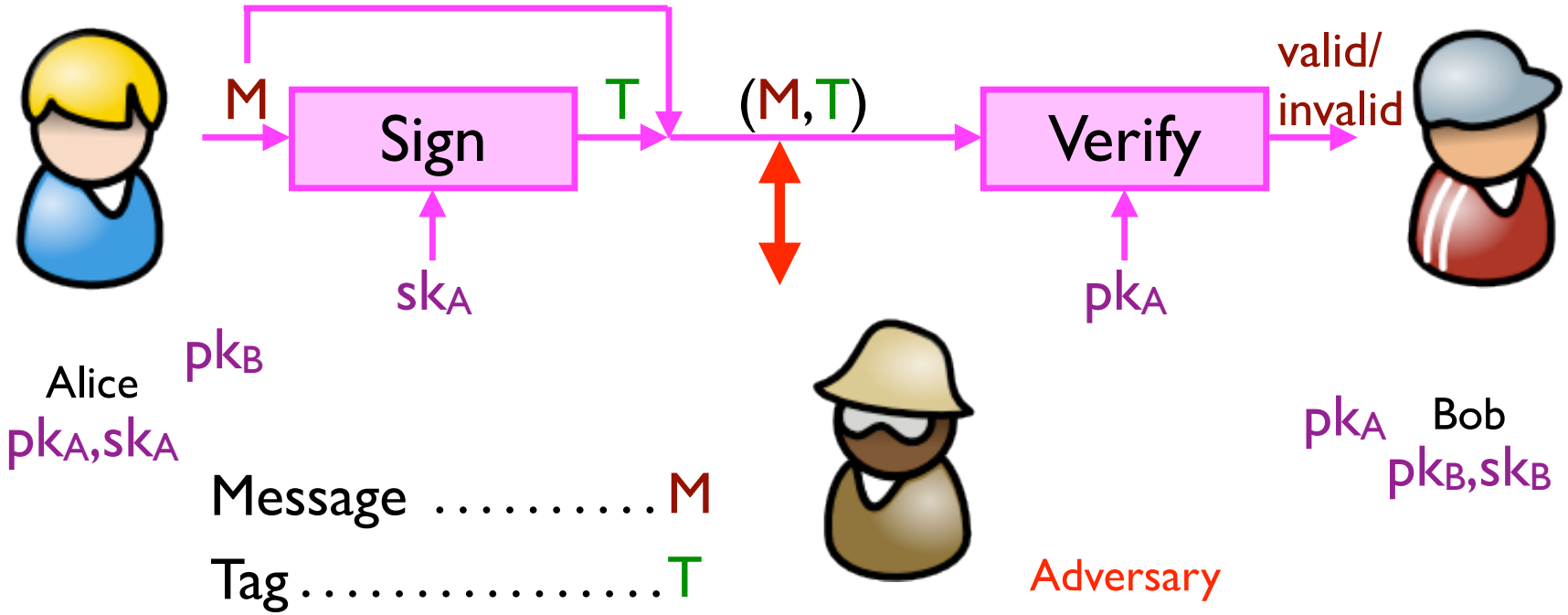
Message authentication schemes: A tool for protecting integrity.

(Also called message authentication codes or MACs.)



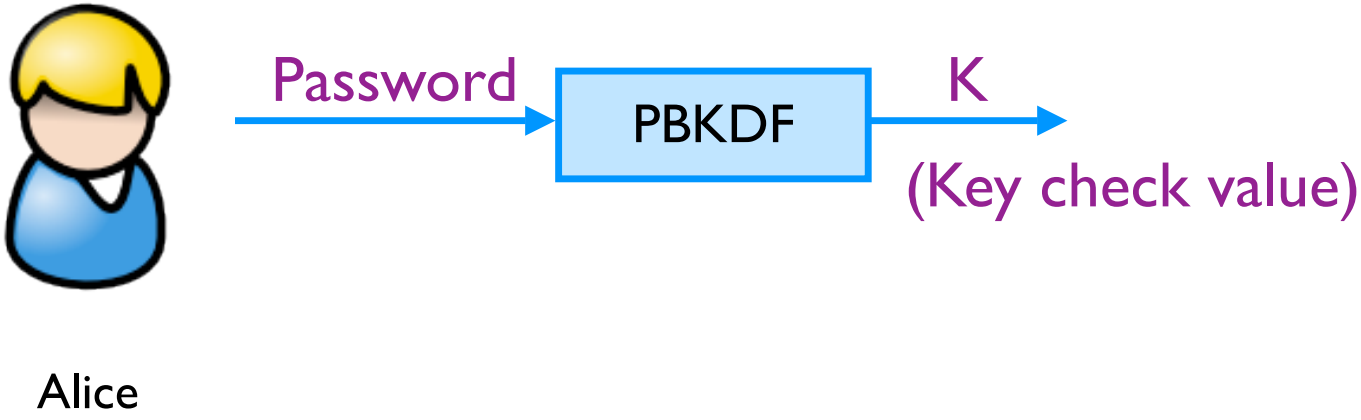
Achieving Integrity (Asymmetric)

Digital signature schemes: A tool for protecting integrity and authenticity.



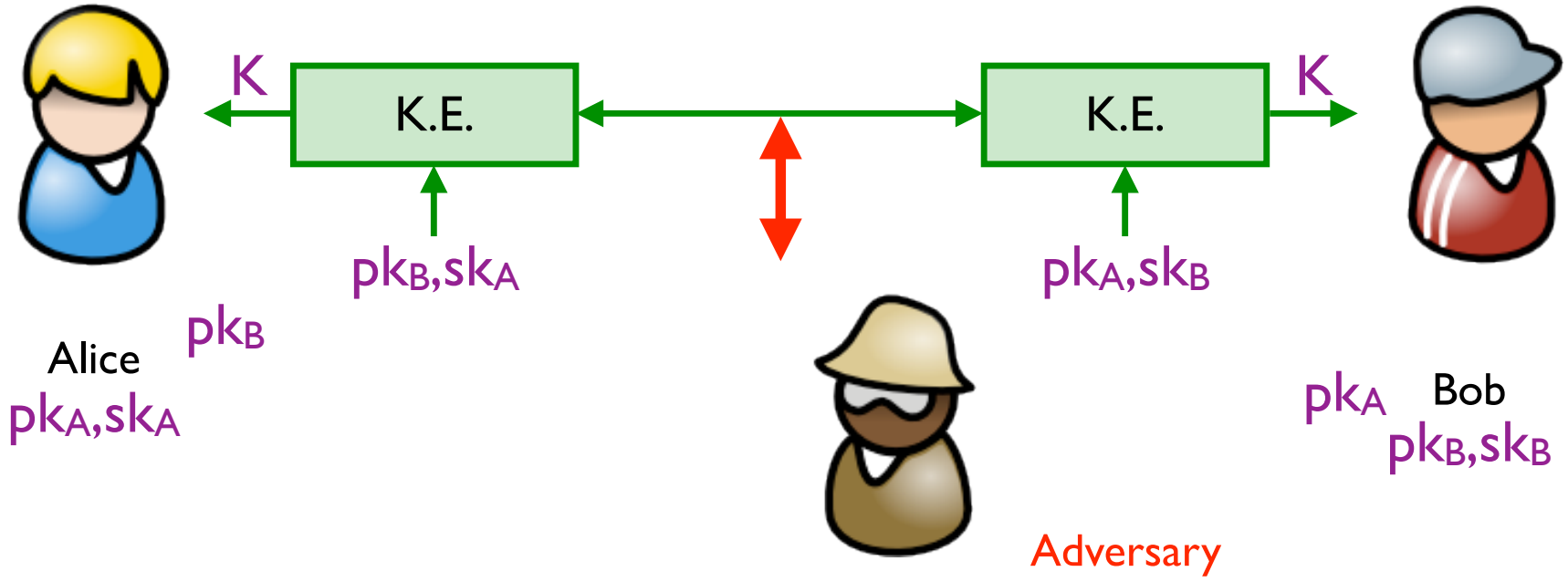
Getting keys: PBKDF

Password-based Key Derivation Functions



Getting keys: Key exchange

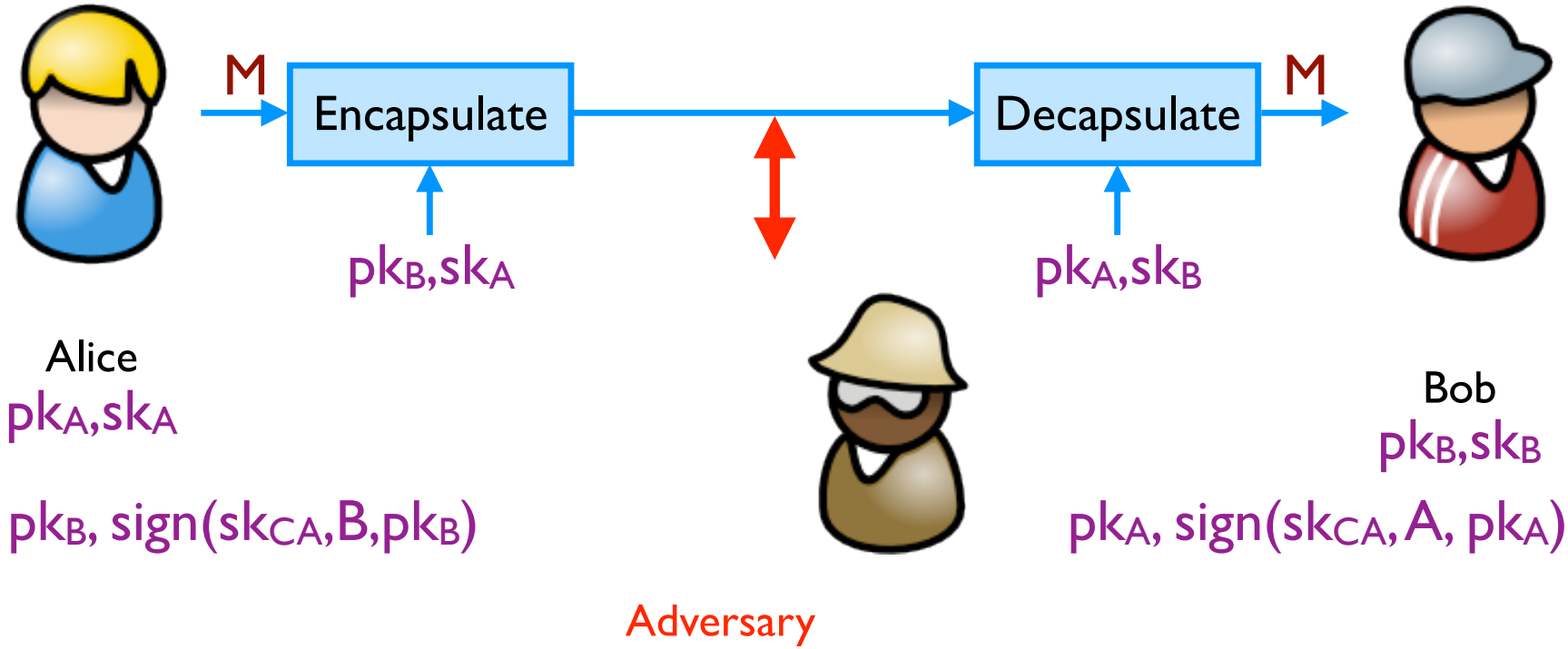
Key exchange protocols: A tool for establishing a share symmetric key



Getting keys: CAs

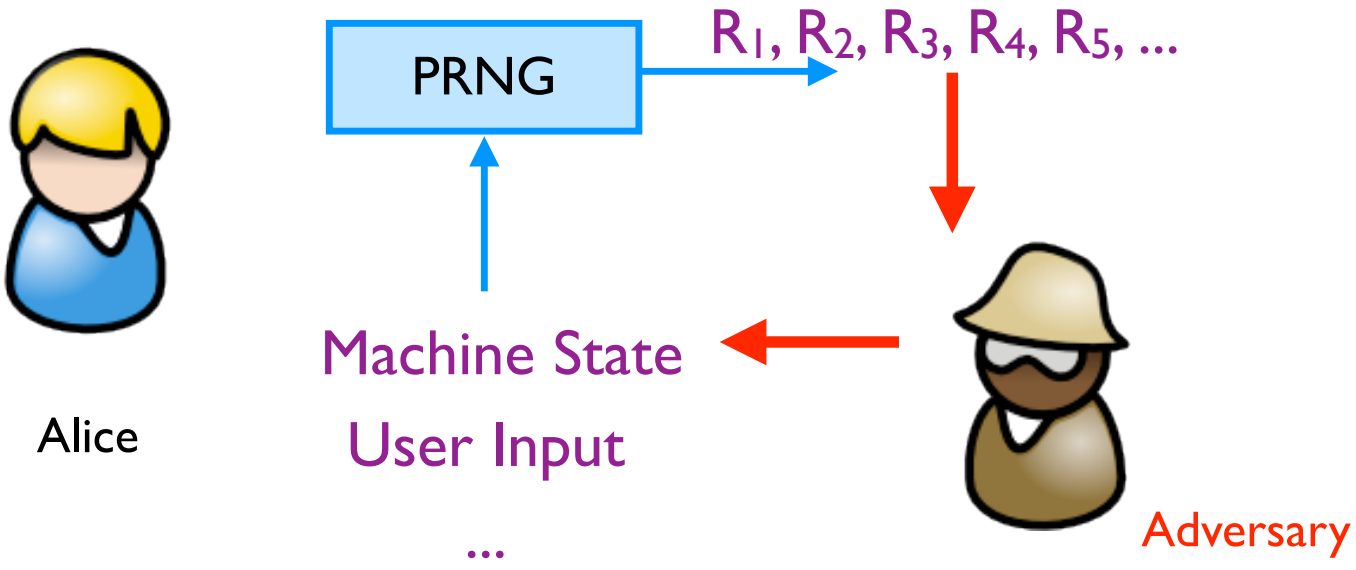
Each party creates a public key pk and a secret key sk.

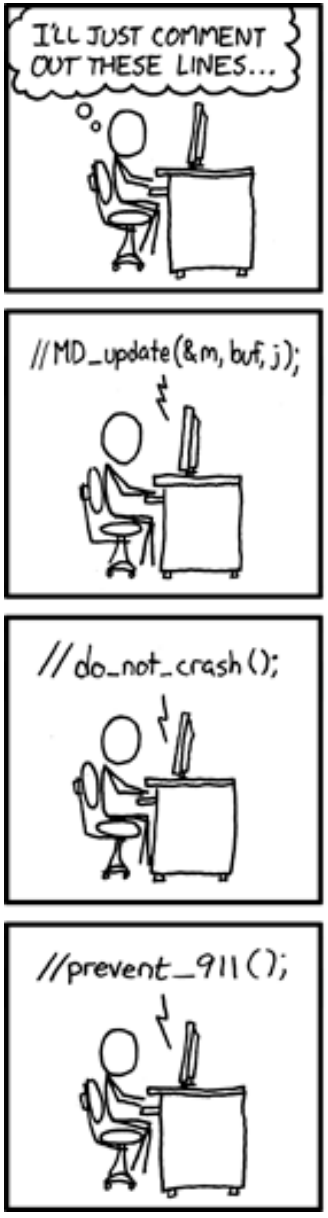
(Public keys signed by a trusted third party: a certificate authority.)



"Random" Numbers

Pseudorandom Number Generators (PRNGs)





IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND"
UBUNTU	TURNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES

Source: XKCD

Kerckhoff's Principle

- Security of a cryptographic object should depend **only** on the secrecy of the secret (privacy) key
- Security should not depend on the secrecy of the algorithm itself.
- Why?

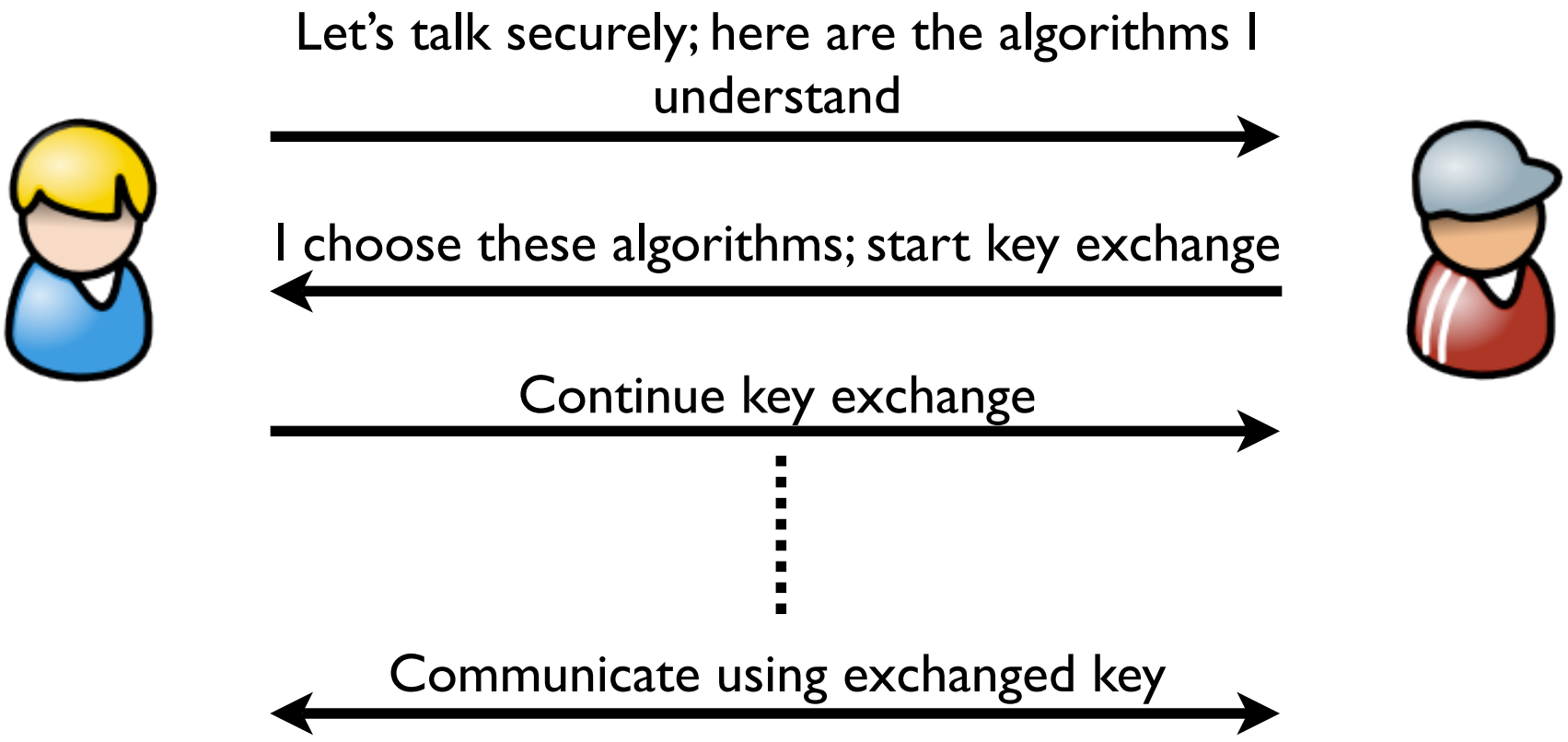
One-way Communications

PGP is a good example

Message encrypted under Bob's public key

Interactive Communications

In many cases, it's probably a good idea to just use a standard protocol/system like SSH, SSL/TLS, etc...



Let's Dive a Bit Deeper

One-way Communications

(*Informal* example; ignoring, e.g., signatures)

1. Alice gets Bob's public key; Alice *verifies* Bob's public key (e.g., via CA)
2. Alice generates random symmetric keys K1 and K2
3. Alice encrypts the message M the key K1; call result C
4. Alice authenticates (MACs) C with key K2; call the result T
5. Alice encrypts K1 and K2 with Bob's public key; call the result D

6. Send D, C, T

(Assume Bob's private key is encrypted on Bob's disk.)

7. Bob takes his password to derive key K3
8. Bob decrypts his private key with key K3
9. Bob uses private key to decrypt K1 and K2
10. Bob uses K2 to verify MAC tag T
11. Bob uses K1 to decrypt C

Interactive Communications

(*Informal* example; details omitted)

1. Alice and Bob exchange public keys and certificates
2. Alice and Bob use CA's public keys to verify certificates and each other's public keys
3. Alice and Bob take their passwords and derive symmetric keys
4. Alice and Bob use those symmetric keys to decrypt and recover their asymmetric private keys.
5. Alice and Bob use their asymmetric private keys and a *key exchange* algorithm to derive a shared symmetric key

(They key exchange process will require Alice and Bob to generate new pseudorandom numbers)

6. Alice and Bob use shared symmetric key to encrypt and authenticate messages

(Last step will probably also use random numbers; will need to rekey regularly; may need to avoid replay attacks,...

History

- Substitution Ciphers
  - Caesar Cipher
- Transposition Ciphers
- Codebooks
- Machines

- Recommended Reading: The Codebreakers by David Kahn and The Code Book by Simon Singh.
  - Military uses
  - Rumrunners
  - ....

Classic Encryption

- Goal: To communicate a secret message
- Start with an *algorithm*
- Caesar cipher (substitution cipher):

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ

GHIJKLMNOPQRSTUVWXYZABCDEF
```

Then add a secret key

- Both parties know that the secret word is "victory":

  ABCDEFGHIJKLMNOPQRSTUVWXYZ

  VICTORYABDEFGHJKLMNPQSUWXZ

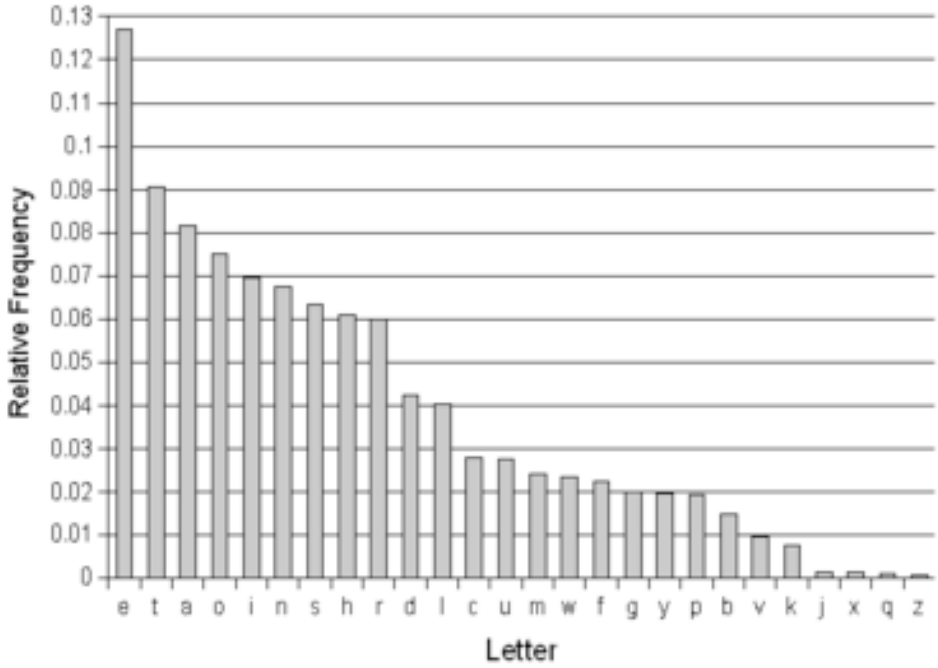
- "state of the art" for thousands of years

Cryptographers vs Cryptanalysts

- A battle that continues today
- Cryptographers try to devise more clever algorithms and keys
- Cryptanalysts search for vulnerabilities
- Early cryptanalysts were linguists:
  - frequency analysis
  - properties of letters

Cryptanalysis and probabilities

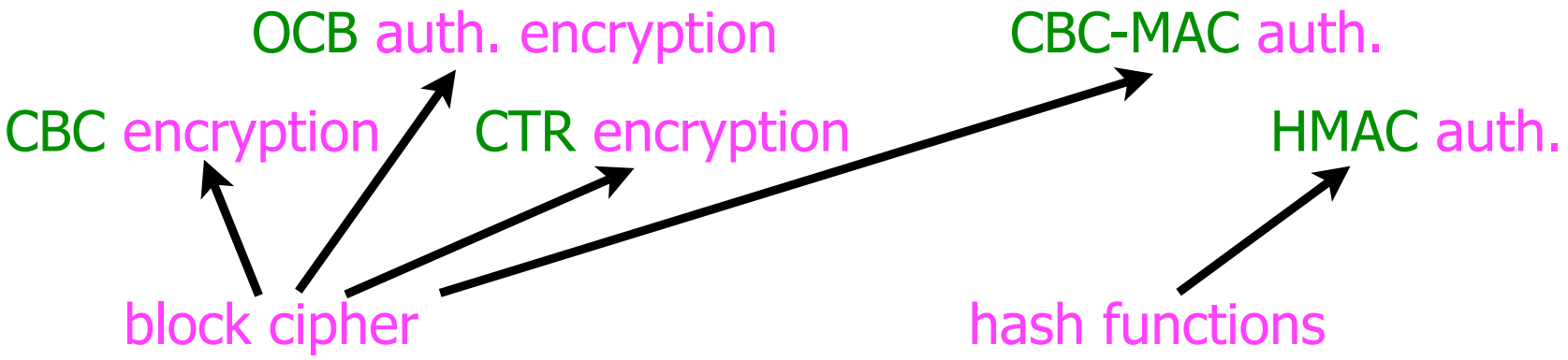
Letter	Frequency
a	8.167%
b	1.492%
c	2.782%
d	4.253%
e	12.702%
f	2.228%
g	2.015%
h	6.094%
i	6.966%
j	0.153%
k	0.772%
l	4.025%



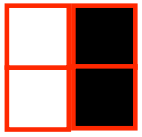
From http://en.wikipedia.org/wiki/Letter_frequencies

How this is achieved today

- Layered approach:
  - Cryptographic primitives, like block ciphers, stream ciphers, and hash functions
  - Cryptographic protocols, like CBC mode encryption, CTR mode encryption, HMAC message authentication
- Public algorithms (Kerckhoff's Principle)
- Security proofs based on assumptions (not this course)



Diversity in Modern Crypto

- **Visual Cryptography**
- Take a black and white bitmap image
- Encode 0 as: 
- Encode 1 as: 
- 1 xor 0 = 0 xor 1 = 1: 
- 1 xor 1 = 0 xor 0 = 0:  or 
- Nice toolkit online here: http://www.cl.cam.ac.uk/~fms27/vck/

See also http://www.cs.washington.edu/homes/yoshi/cs4hs/cse-vc.html