CSE 484 (Winter 2011)

Software Security Design Principles
+
Intro to Crypto

Tadayoshi Kohno

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

Lab 1

- Deadline extended to Feb 2 (Wednesday)

Goals for Today

- Defensive Approaches
- Cryptography Overview

Principles

- Check inputs

Principles

- Least privilege

Principles

- Check all return values

Principles

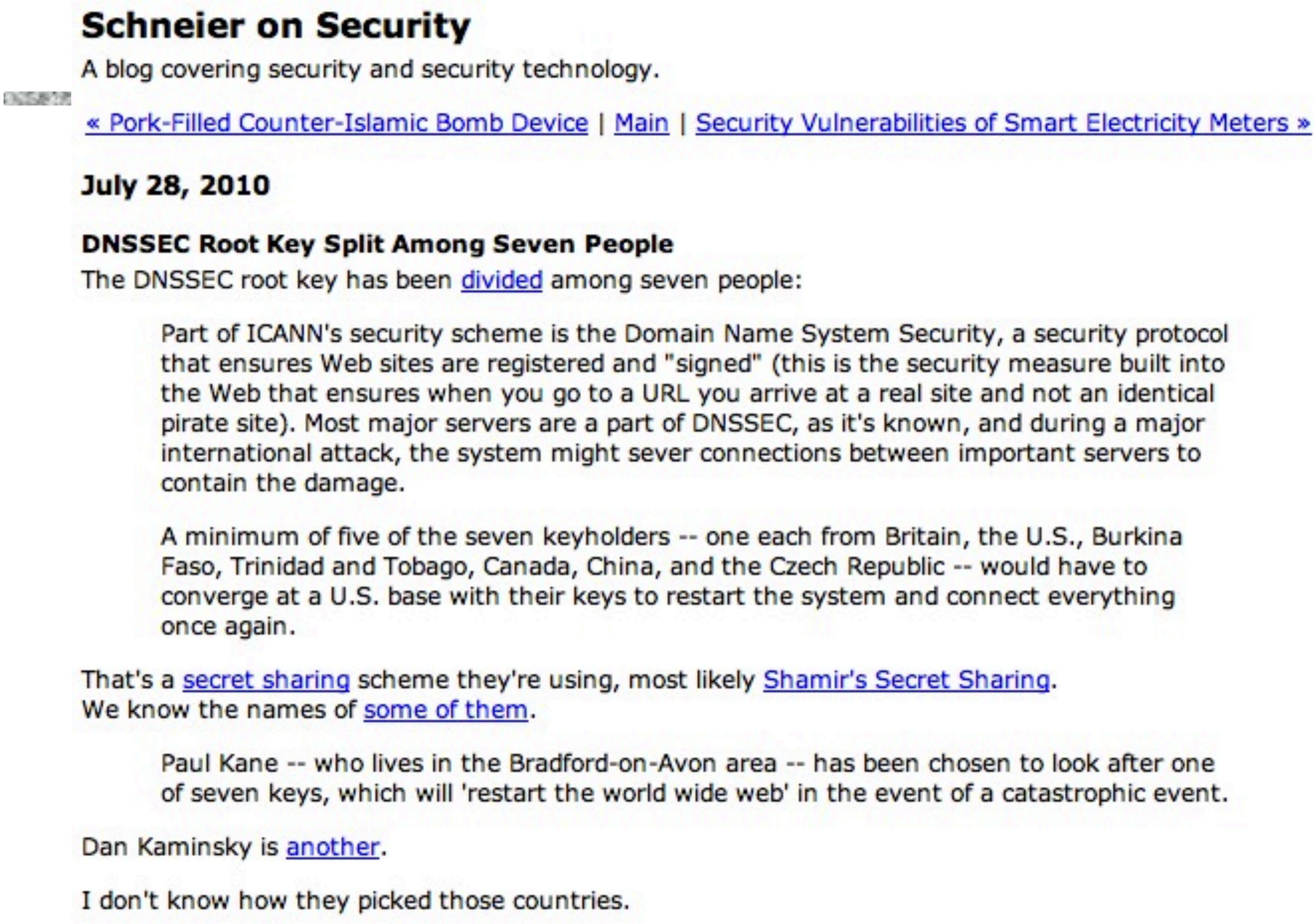
- Securely clear memory (passwords, keys, etc)

Principles

- Failsafe defaults

Principles

- Defense in Depth
- Also
  - Prevent
  - Detect
  - Deter



Schneier on Security

A blog covering security and security technology.

« Pork-Filled Counter-Islamic Bomb Device | Main | Security Vulnerabilities of Smart Electricity Meters »

July 28, 2010

DNSSEC Root Key Split Among Seven People

The DNSSEC root key has been divided among seven people:

> Part of ICANN's security scheme is the Domain Name System Security, a security protocol that ensures Web sites are registered and "signed" (this is the security measure built into the Web that ensures when you go to a URL you arrive at a real site and not an identical pirate site). Most major servers are a part of DNSSEC, as it's known, and during a major international attack, the system might sever connections between important servers to contain the damage.
>
> A minimum of five of the seven keyholders -- one each from Britain, the U.S., Burkina Faso, Trinidad and Tobago, Canada, China, and the Czech Republic -- would have to converge at a U.S. base with their keys to restart the system and connect everything once again.

That's a secret sharing scheme they're using, most likely Shamir's Secret Sharing.
We know the names of some of them.

> Paul Kane -- who lives in the Bradford-on-Avon area -- has been chosen to look after one of seven keys, which will 'restart the world wide web' in the event of a catastrophic event.

Dan Kaminsky is another.

I don't know how they picked those countries.

Principles

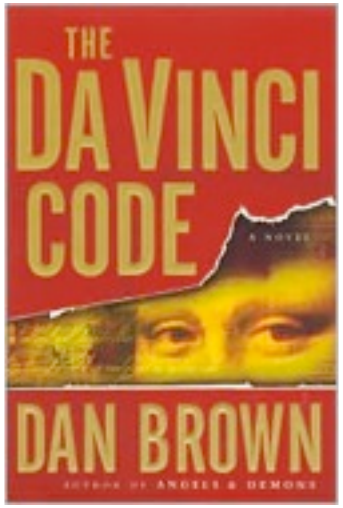
- Reduce size of TCB
- Simplicity
- Modularity

Vulnerability Analysis and Disclosure

- What do you do if you’ve found a security problem in a real system?
- Say
  - A commercial website?
  - UW grade database?
  - iPhone?
  - Boeing 787?

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.



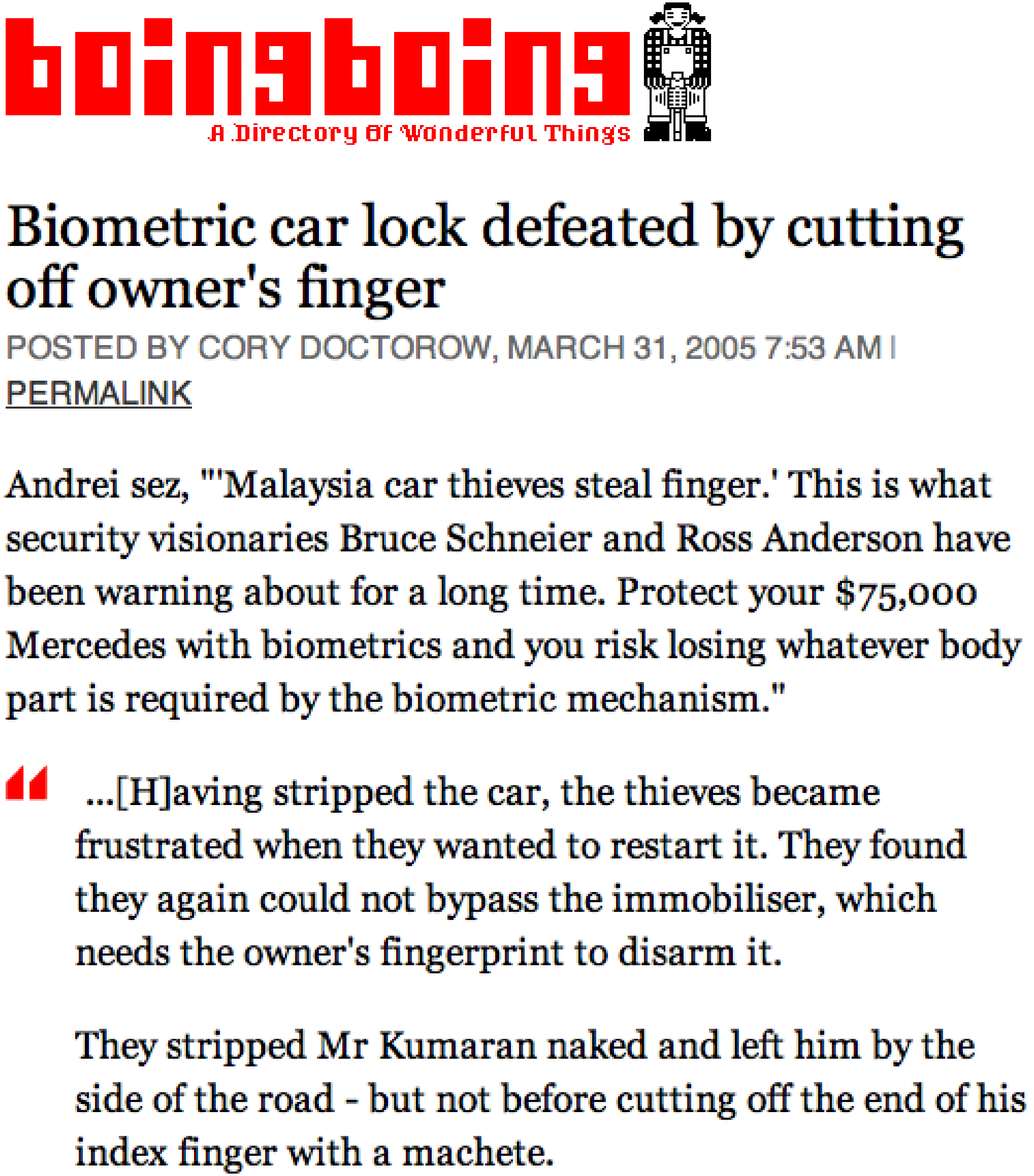
Images from Wikipedia and Barnes and Noble

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)
  - Crypto failures may not be (immediately) detected
- Cryptography helps after you've identified your threat model and goals

Improved se

- RFIDs in car ke
  - RFIDs in car ke
  - Result: Car ja



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)

- This is the key pad on my office safe.
- Inside my safe is a copy of 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

Image from profmason.com

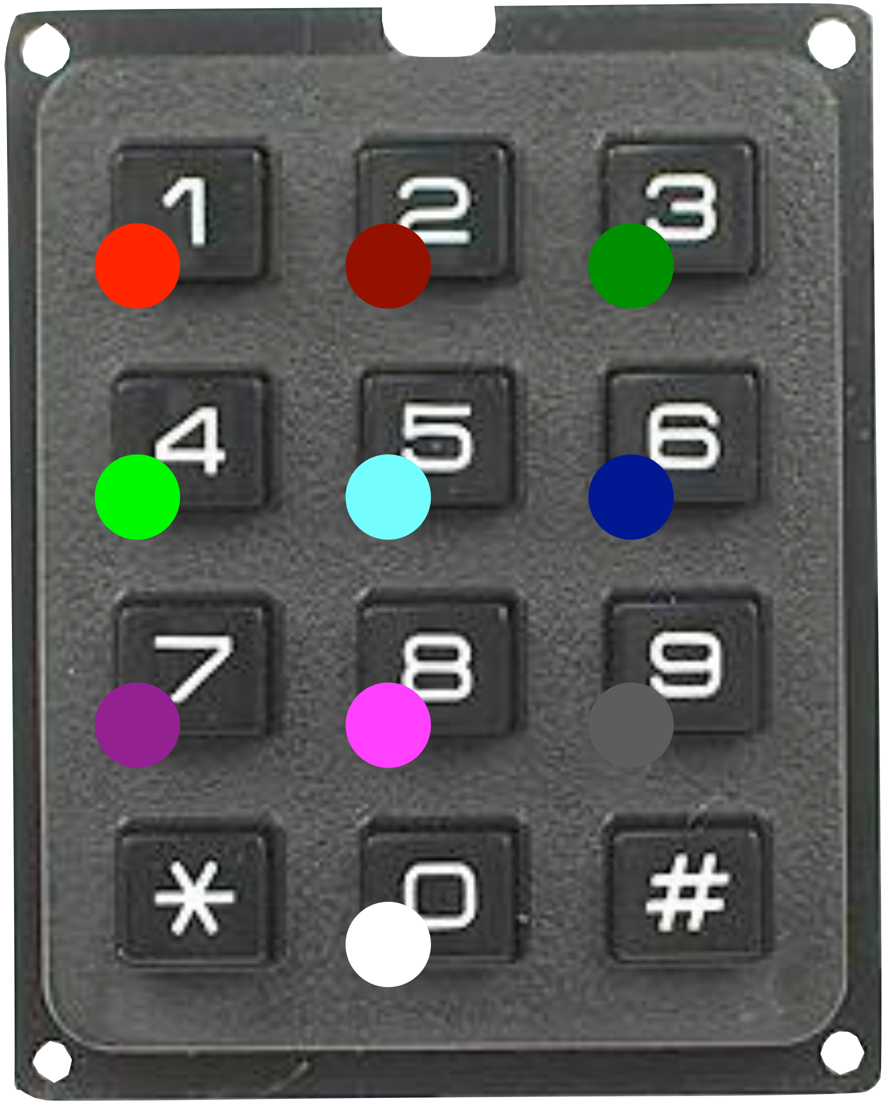
Key Entry Pad (4-digit PIN)

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 × (9999 choose 2) possible choices contain the correct PIN
  - So success probability is 3 / 10000

Key Entry Pad (4-digit PIN)



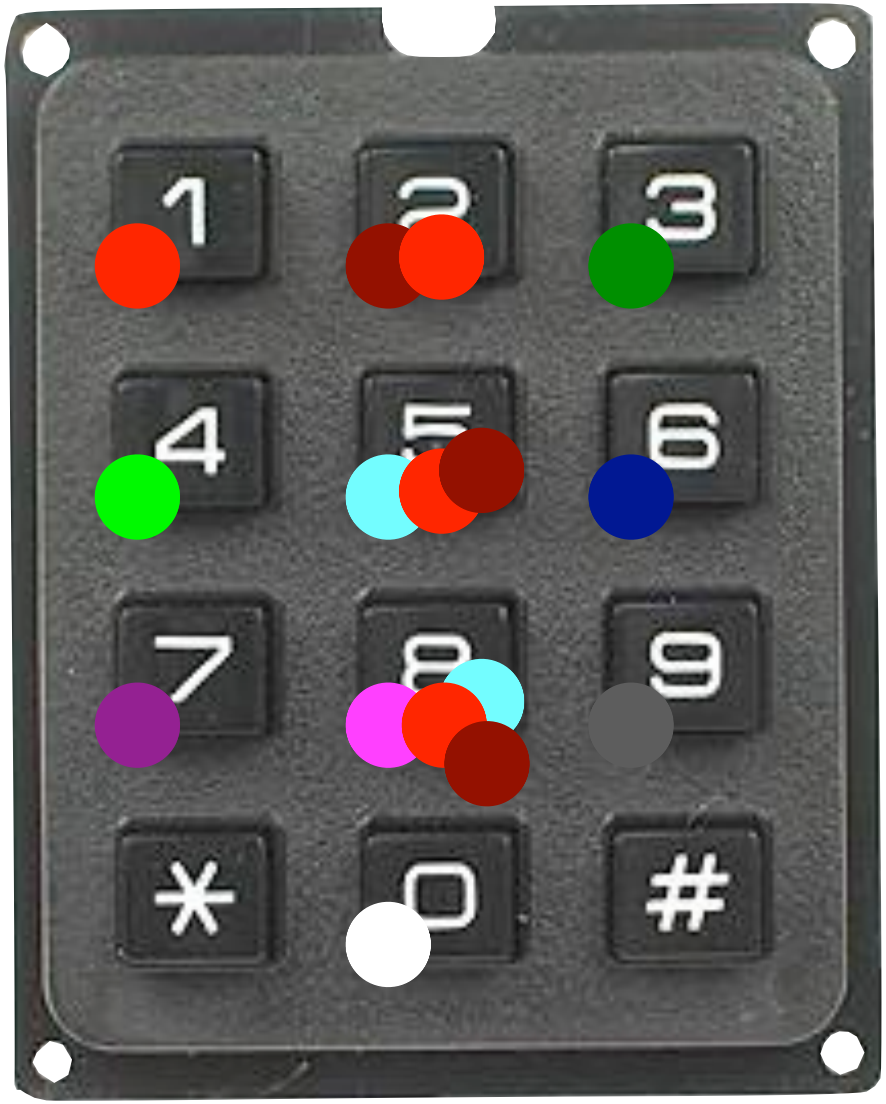
- Could you do better at guessing the PIN?

- 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)



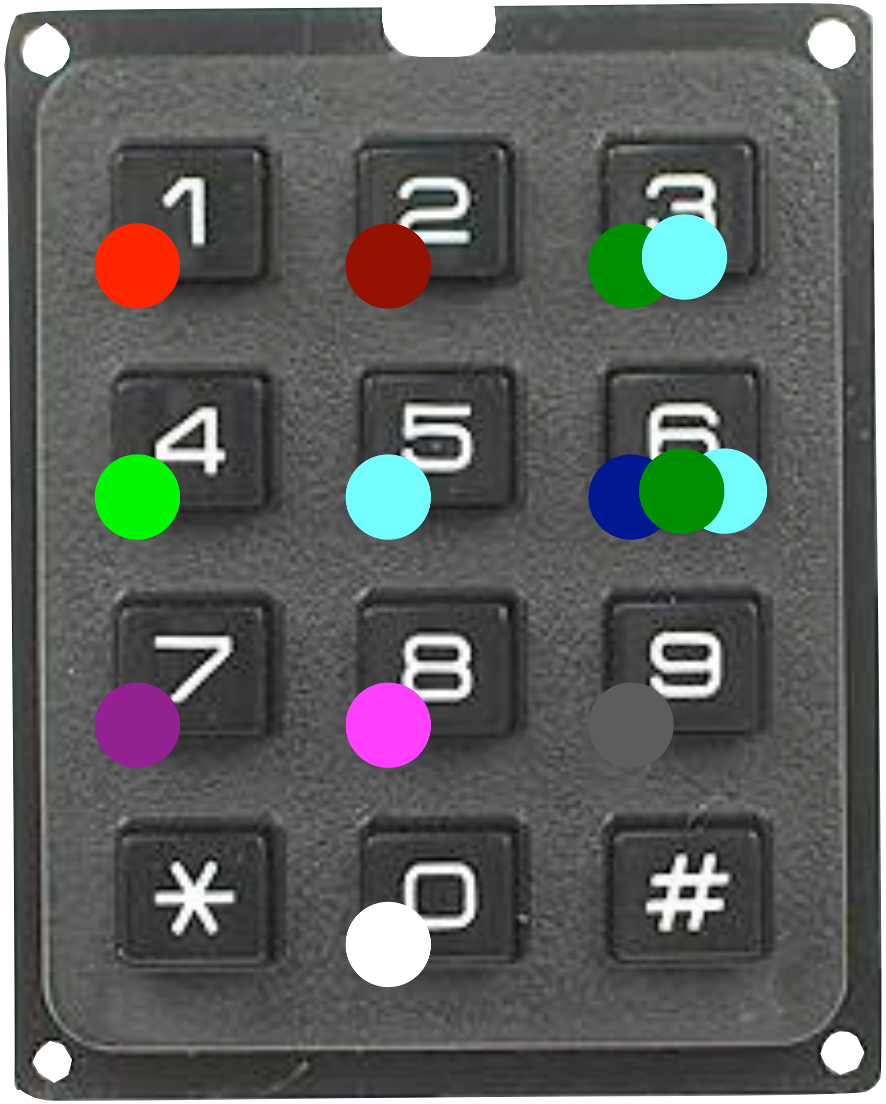
- Could you do better at guessing the PIN?

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

Image from profmason.com

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

Key Entry Pad (4-digit PIN)



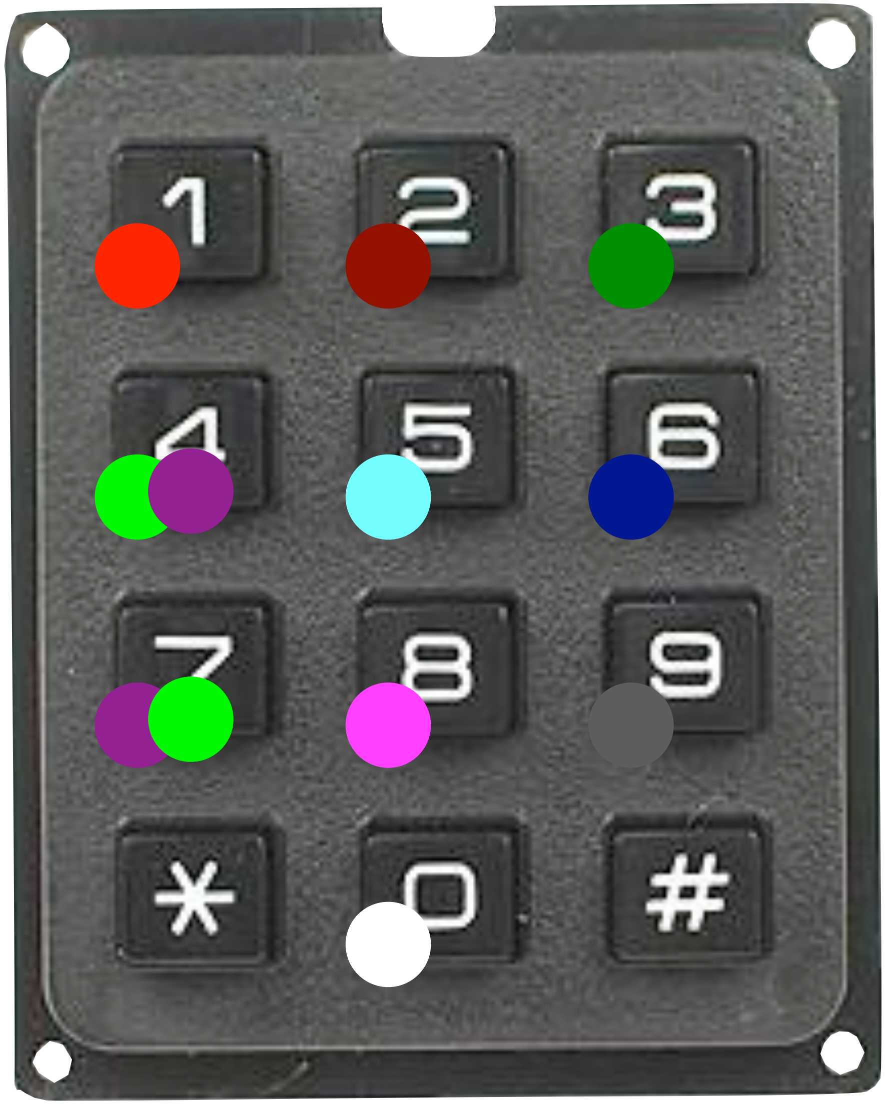
- Could you do better at guessing the PIN?

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

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

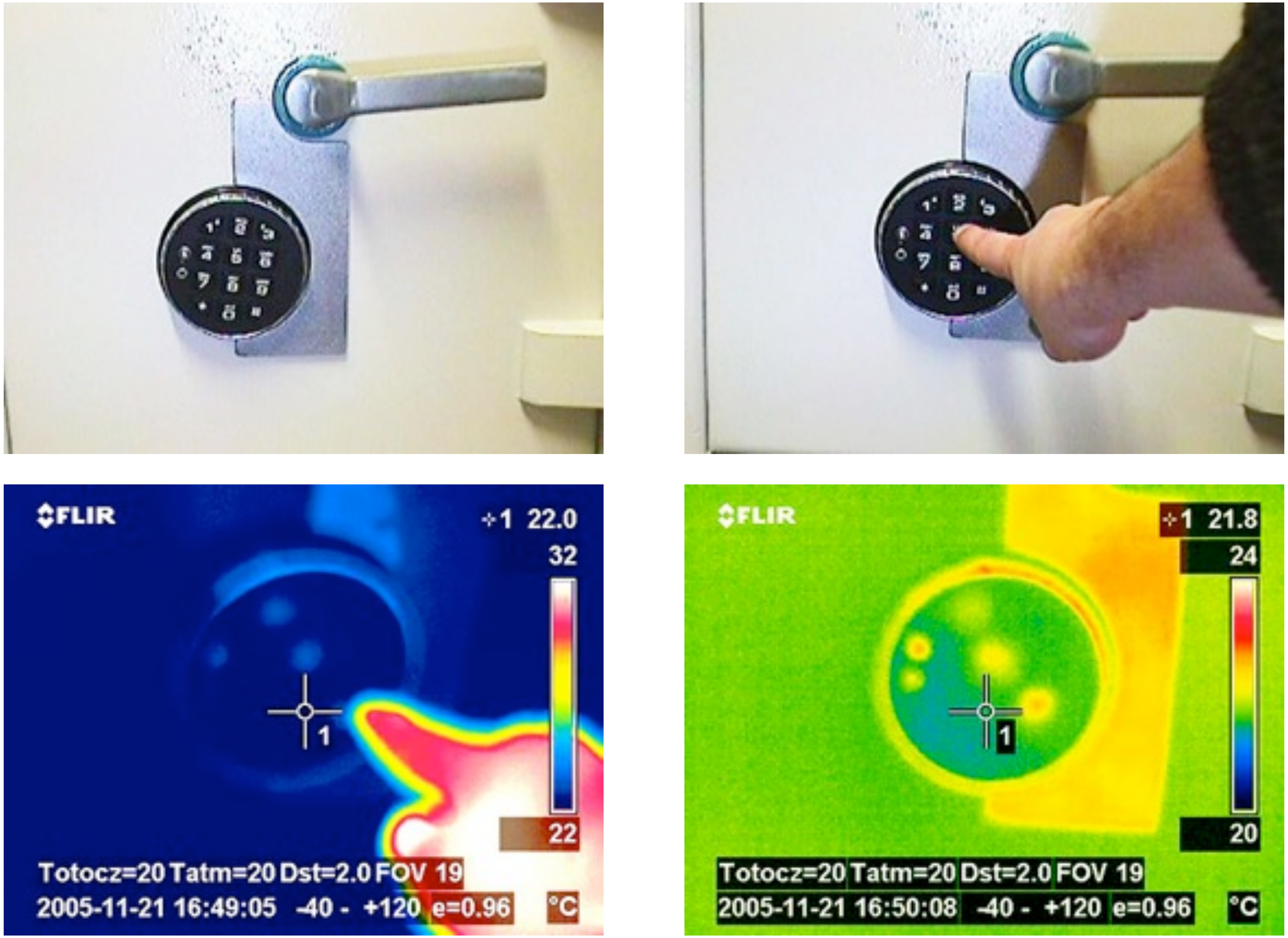
Lesson: Consider the complete system, physical security, etc

Lesson: Think outside the box

Image from profmason.com

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

Thermal Patterns

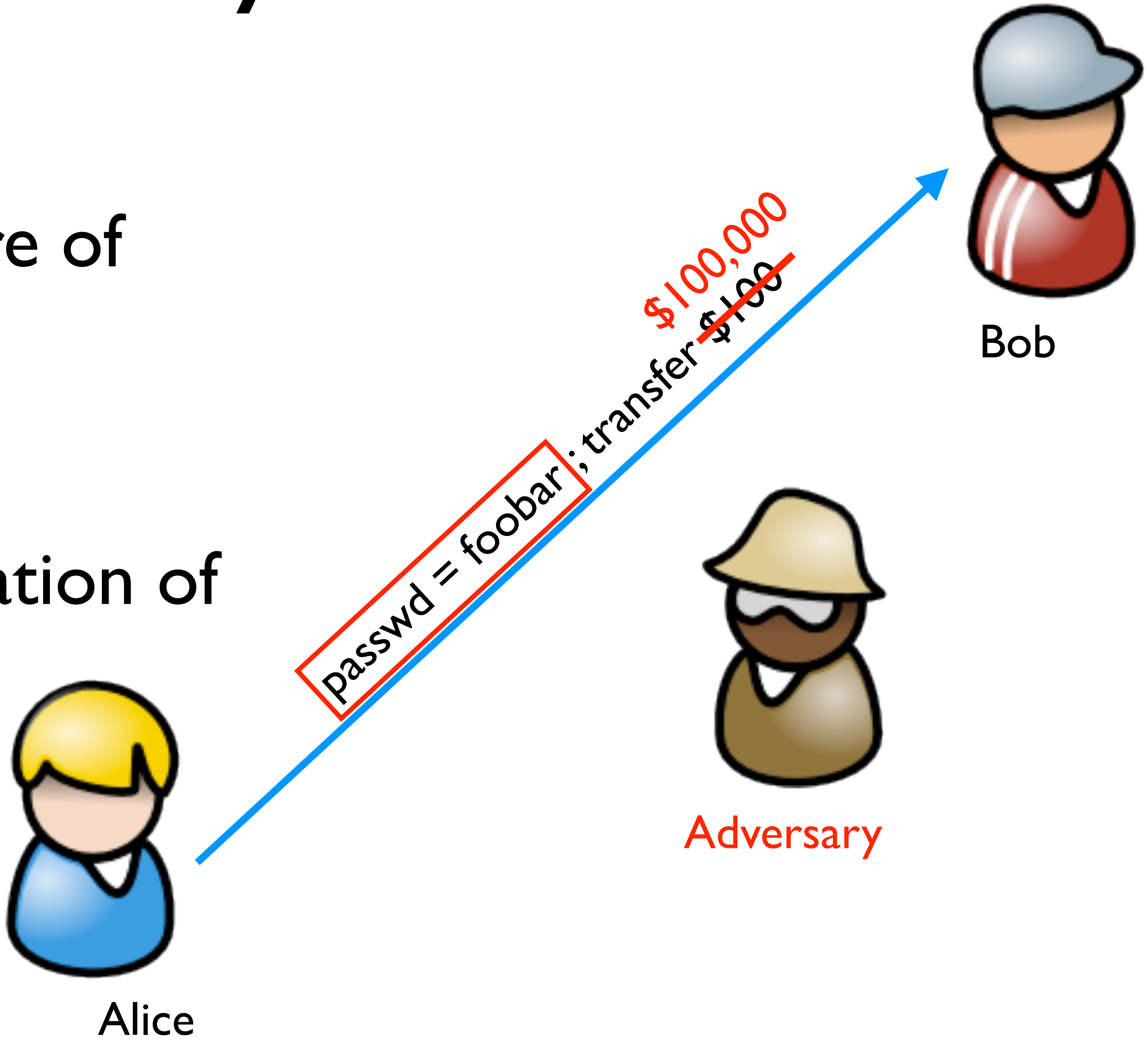

FLIR
1 22.0
32
22
1
Totocz=20 Tatm=20 Dst=2.0 FOV 19
2005-11-21 16:49:05 -40 - +120 e=0.96 °C
FLIR
1 21.8
24
20
1
Totocz=20 Tatm=20 Dst=2.0 FOV 19
2005-11-21 16:50:08 -40 - +120 e=0.96 °C

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

Common Communication Security Goals

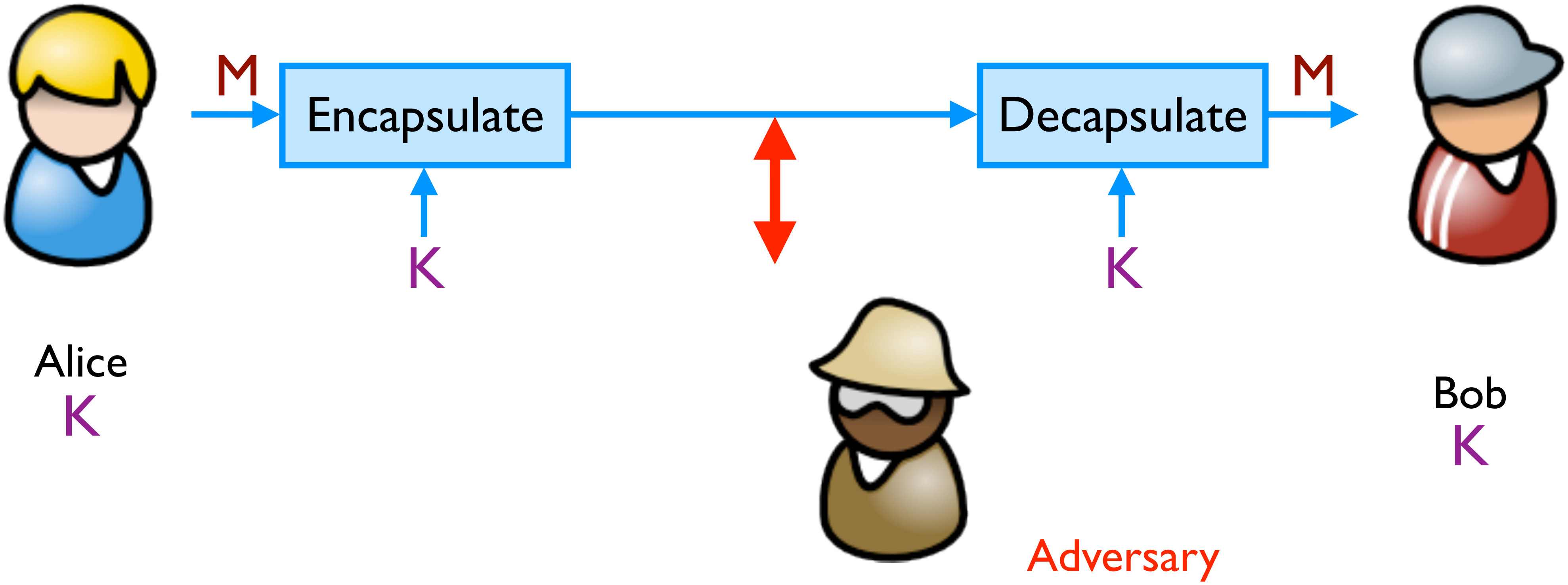
Privacy of data
Prevent exposure of information

Integrity of data
Prevent modification of information



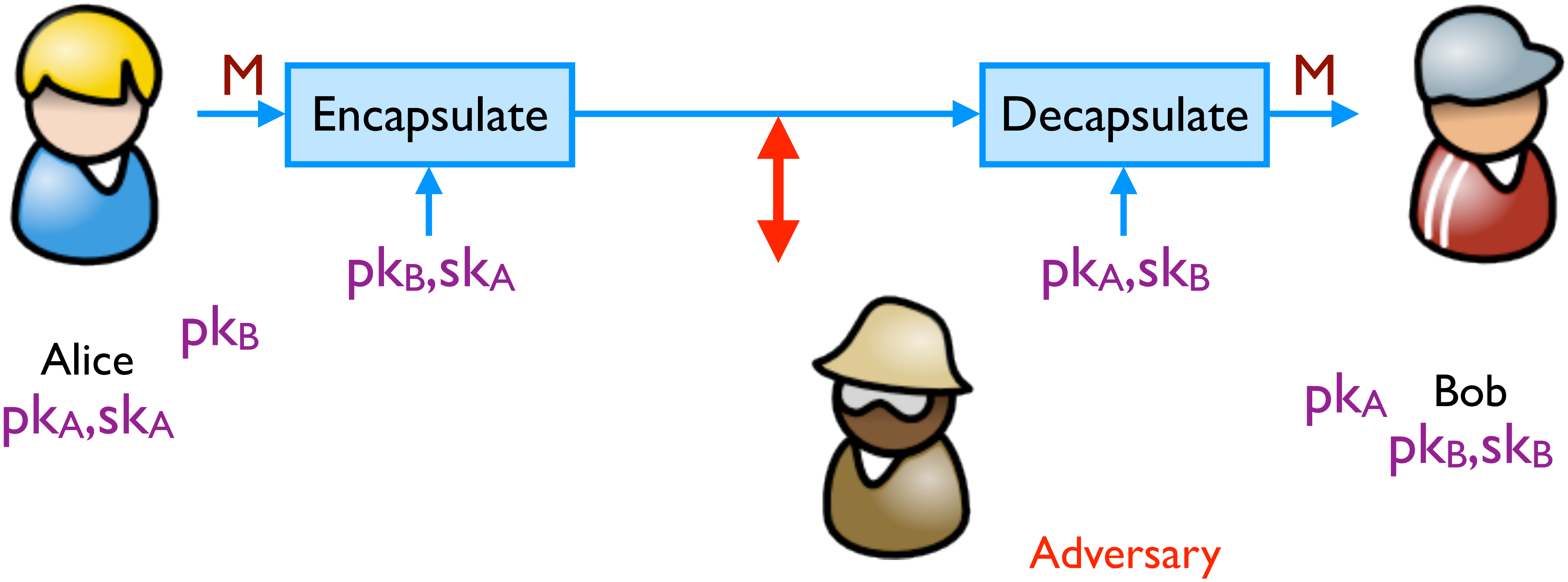
Symmetric Setting

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.



M

Encapsulate

Decapsulate

M

pk_B, sk_A

pk_A, sk_B

Alice

pk_B

pk_A, sk_A

Adversary

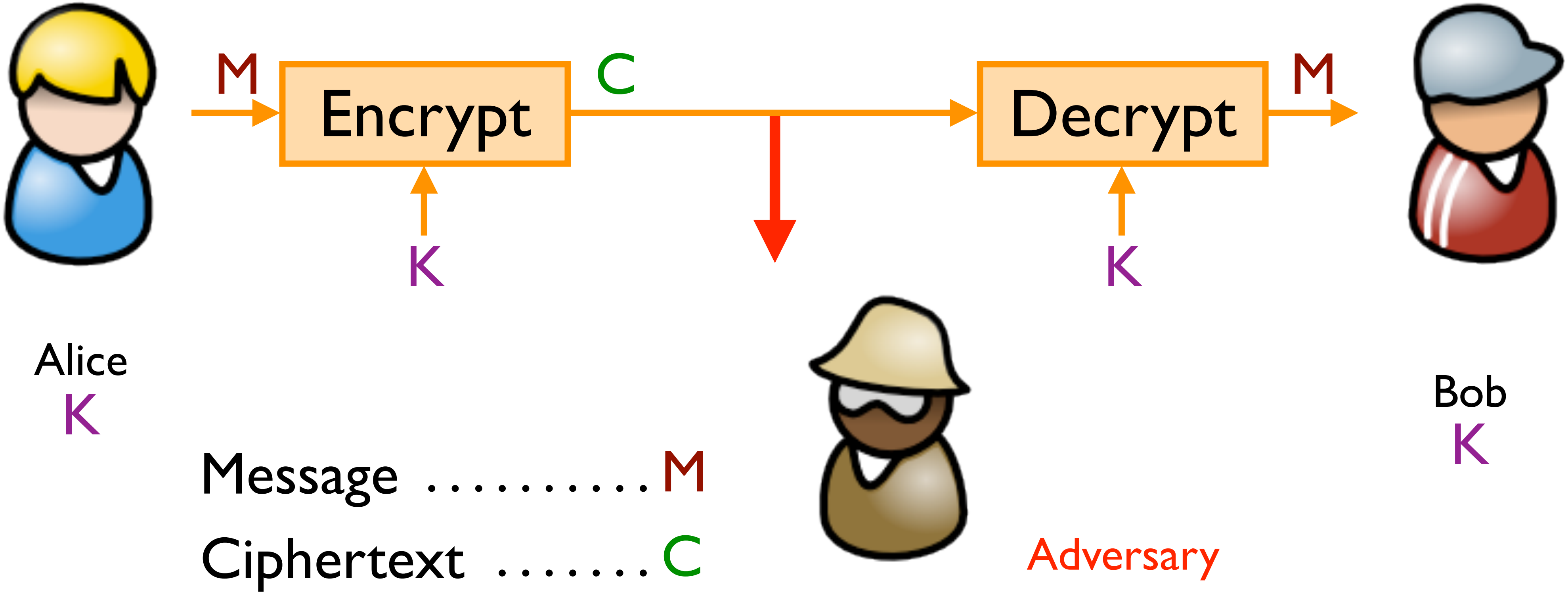
pk_A

Bob

pk_B, sk_B

Achieving Privacy (Symmetric)

Encryption schemes: A tool for protecting privacy.



M

Encrypt

C

Decrypt

M

K

K

Alice
K

Bob
K

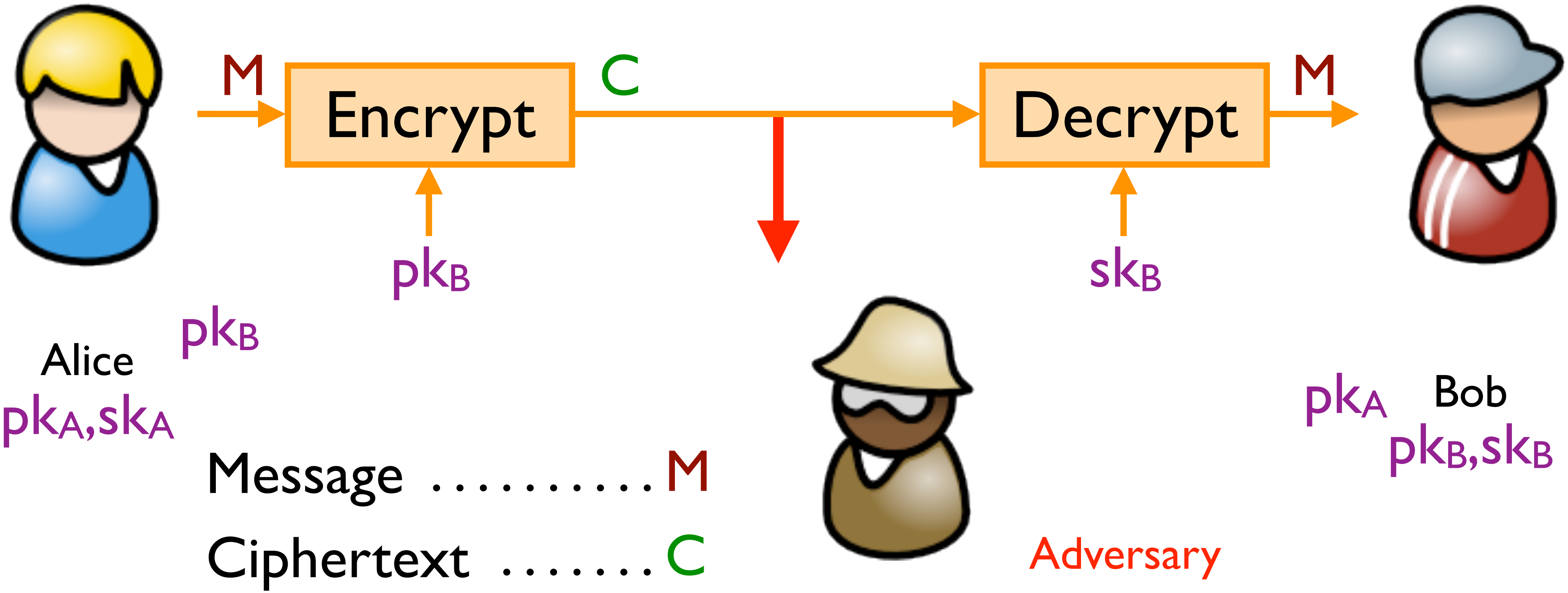
Adversary

Message . . . . M

Ciphertext C

Achieving Privacy (Asymmetric)

Encryption schemes: A tool for protecting privacy.



M

Encrypt

C

Decrypt

M

pk_B

sk_B

pk_B

Alice

pk_A, sk_A

Message . . . . M

Ciphertext C

Adversary

pk_A

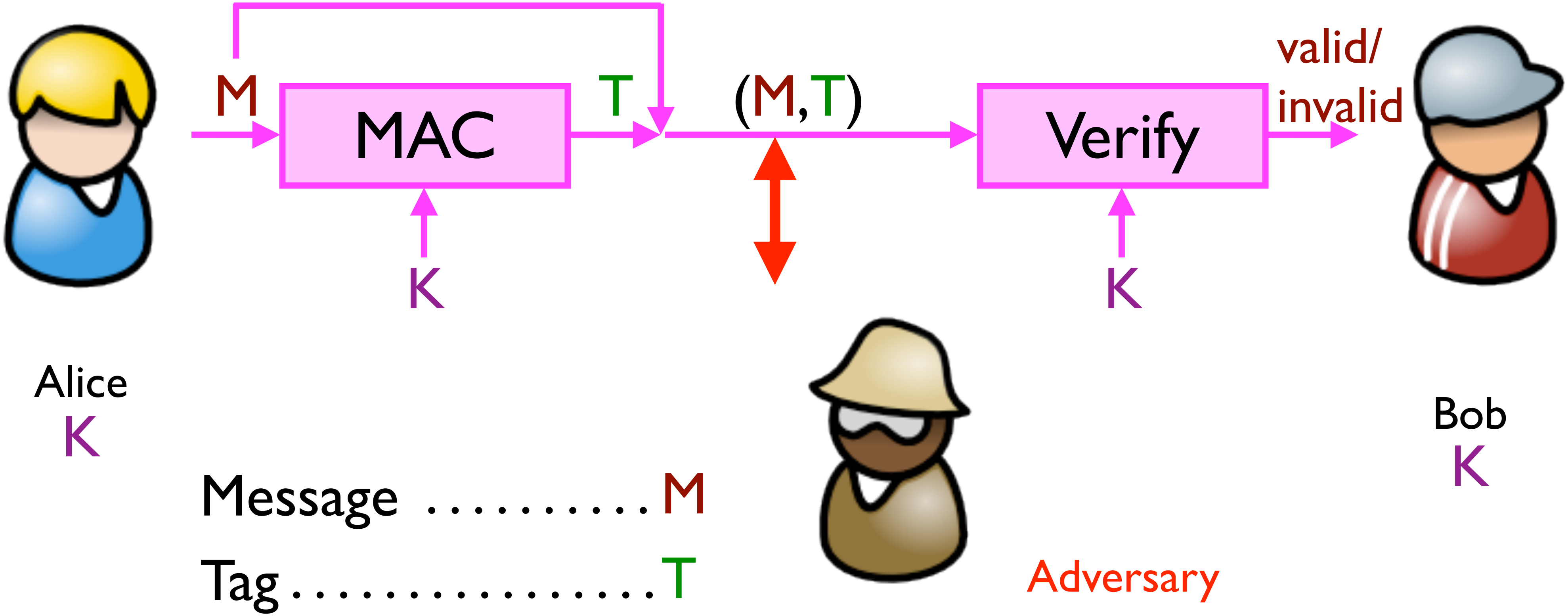
Bob

pk_B, sk_B

Achieving Integrity (Symmetric)

Message authentication schemes: A tool for protecting integrity.

(Also called message authentication codes or MACs.)

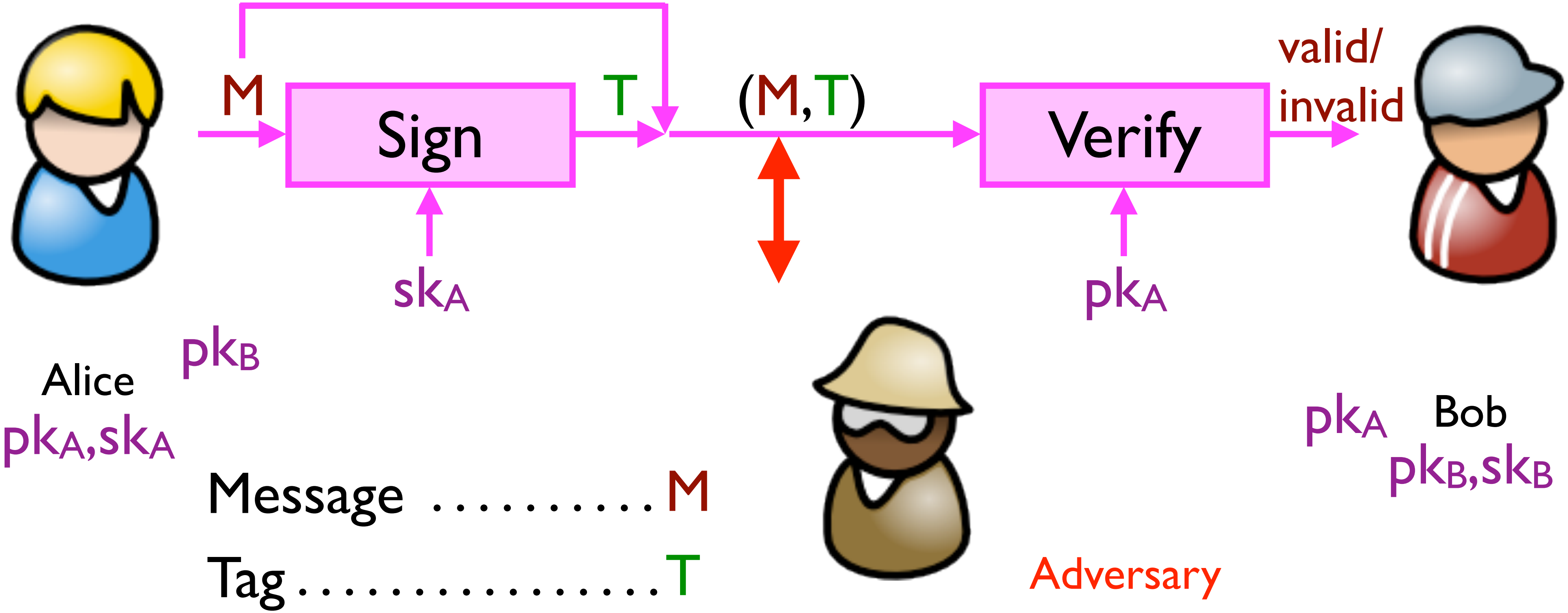


Message . . . . M

Tag . . . . T

Achieving Integrity (Asymmetric)

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



M

Sign

T

(M,T)

Verify

valid/ invalid

sk_A

pk_A

Alice

pk_A, sk_A

pk_B

Bob

pk_B, sk_B

pk_A

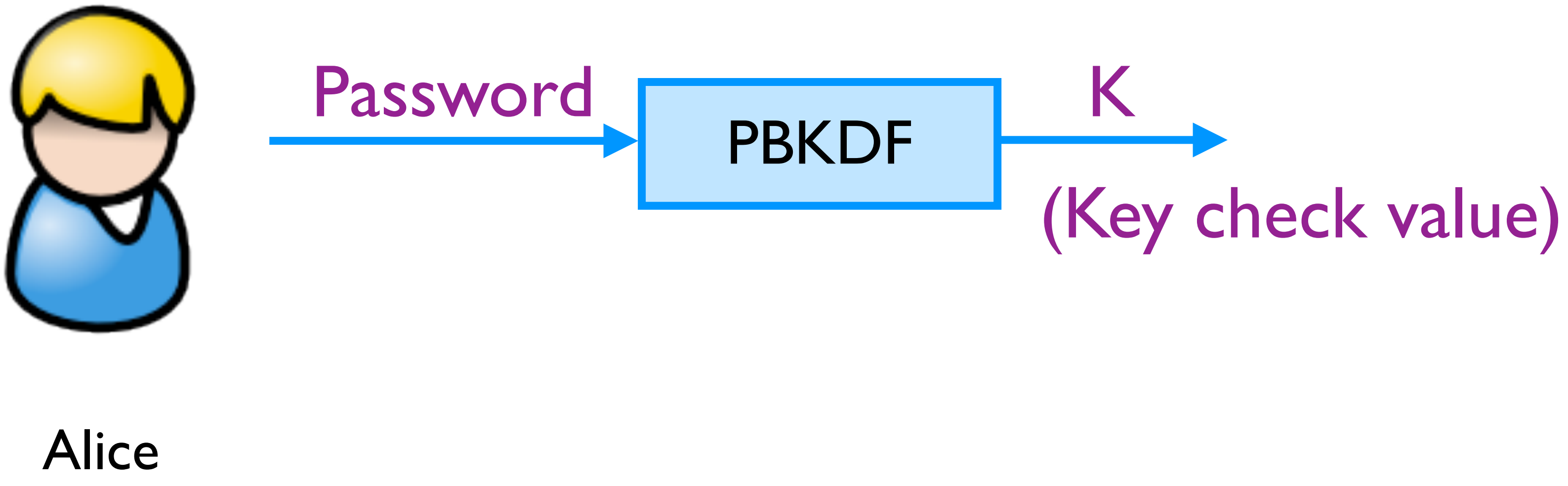
Adversary

Message . . . . M

Tag . . . . T

Getting keys: PBKDF

Password-based Key Derivation Functions


Password
PBKDF
K
(Key check value)
Alice