CSE 484 / CSE M 584: Computer Security and Privacy

Finish Software Security / Intro to Cryptography

Spring 2015

Franziska (Franzi) Roesner
franzi@cs.washington.edu

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

Last Time: Software Security

- Principles:
  - Check inputs, Check all return values, Least privilege, Securely clear memory (passwords, keys, etc.), Failsafe defaults, Defense in depth, NOT security through obscurity, Reduce size of trusted computing base (TCB), Minimize attack surface, Use vetted components, Security by design
  - Simplicity, modularity
    - But: Be careful at interface boundaries!
  - Open design? Open source? Closed source?
    - Different perspectives

Does Open Source Help?

- Different perspectives…
- Happy example:
  - Linux kernel backdoor attempt thwarted (2003)
    (http://www.freedom-to-tinker.com/?p=472)
- Sad example:
  - Heartbleed (2014)
    - Vulnerability in OpenSSL that allowed attackers to read arbitrary memory from vulnerable servers (including private keys)

Vulnerability Analysis and Disclosure

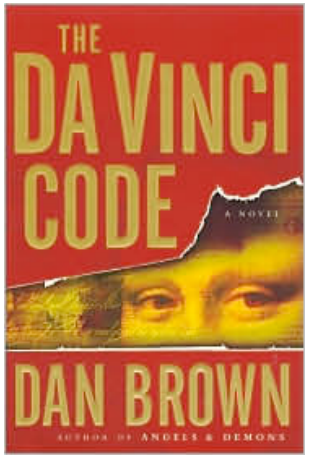
- What do you do if you've found a security problem in a real system?
- Say
  - A commercial website?
  - UW grade database?
  - Boeing 787?
  - TSA procedures?

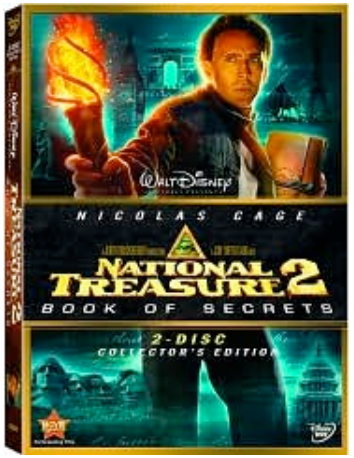
Abj sbe fbzr pelcgbtencul!

Now for some cryptography!

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.

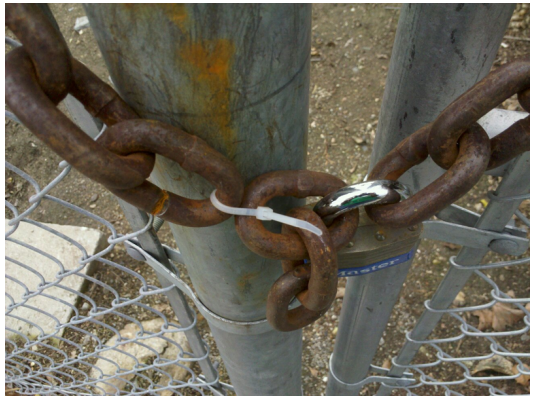




Images from Wikipedia and Barnes and Noble

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
  - Famous quote: "Those who think that cryptography can solve their problems doesn't understand cryptography and doesn't understand their problems."



Improved Security, Increased Risk

- RFIDs in car keys:
  - RFIDs in car keys make it harder to hotwire a car
  - Result: Car jackings increased

Improved Se

- RFIDs in car keys:
  - RFIDs in car keys
  - Result: Car jackin

boingboing
A Directory Of Wonderful Things

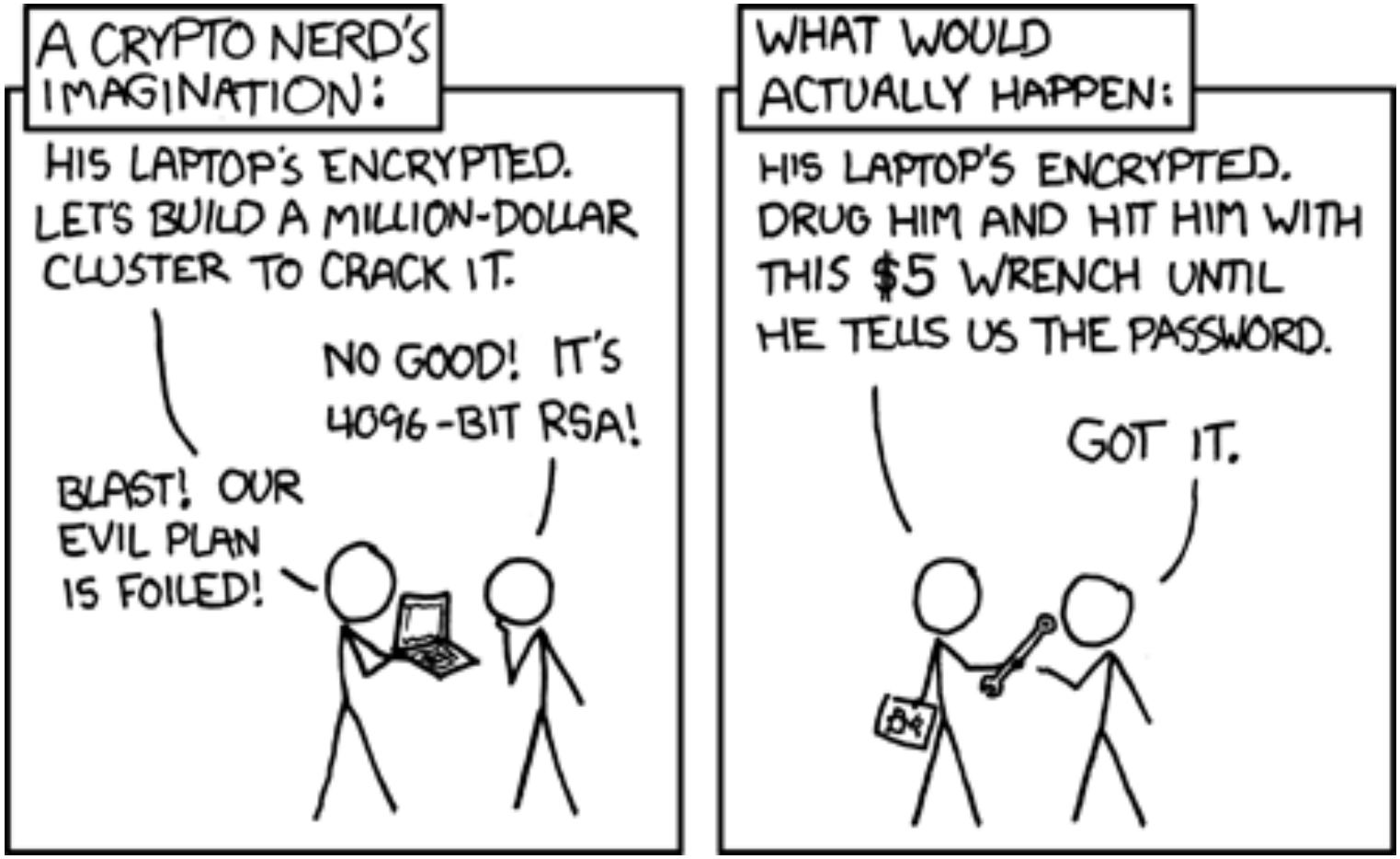
Biometric car lock defeated by cutting off owner's finger

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.

XKCD: http://xkcd.com/538/



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 final exam.
- How long would it take 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 · (9999 choose 2) possible choices contain the correct PIN
  - So success probability is 3 / 10000

Key Entry Pad (4-digit PIN)

Image from profmason.com

- Could you do better at guessing the PIN?
- Answer (*chemical* combinatorics):
  - Put different chemical on each key (NaCl, KCl, LiCl, …)

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

Key Entry Pad (4-digit PIN)

Image from profmason.com

- 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

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

Key Entry Pad (4-digit PIN)

Image from profmason.com

- 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

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

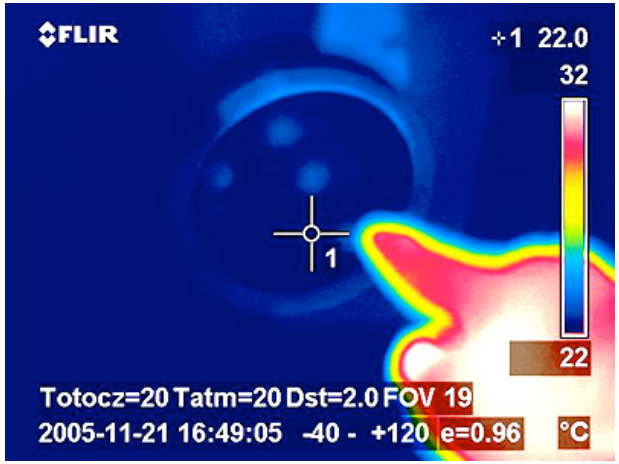
Key Entry Pad (4-digit PIN)

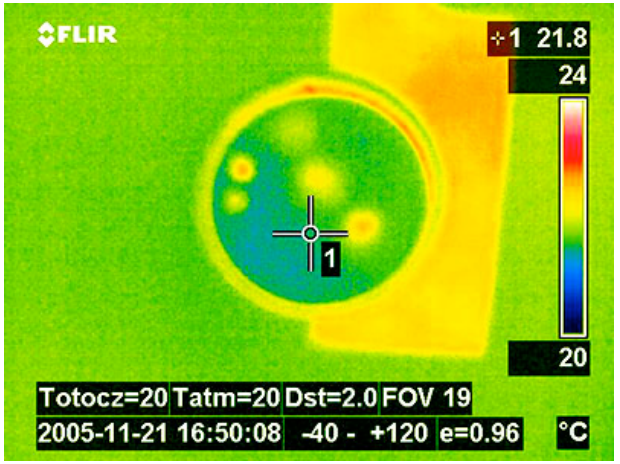
Image from profmason.com

- 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

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

Thermal Patterns

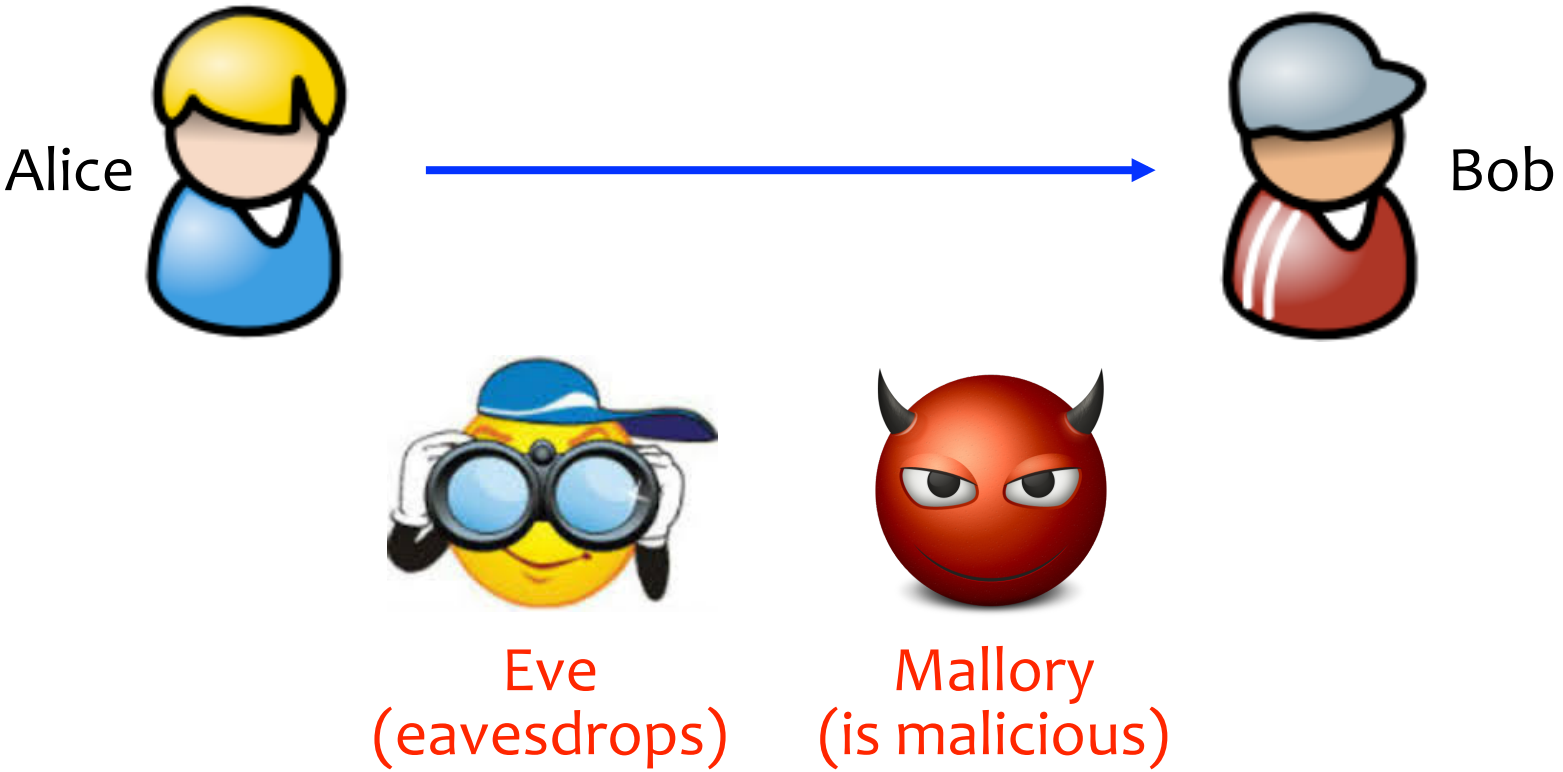




Images from http://lcamtuf.coredump.cx/tsafe/

Alice and Bob

- Archetypical characters



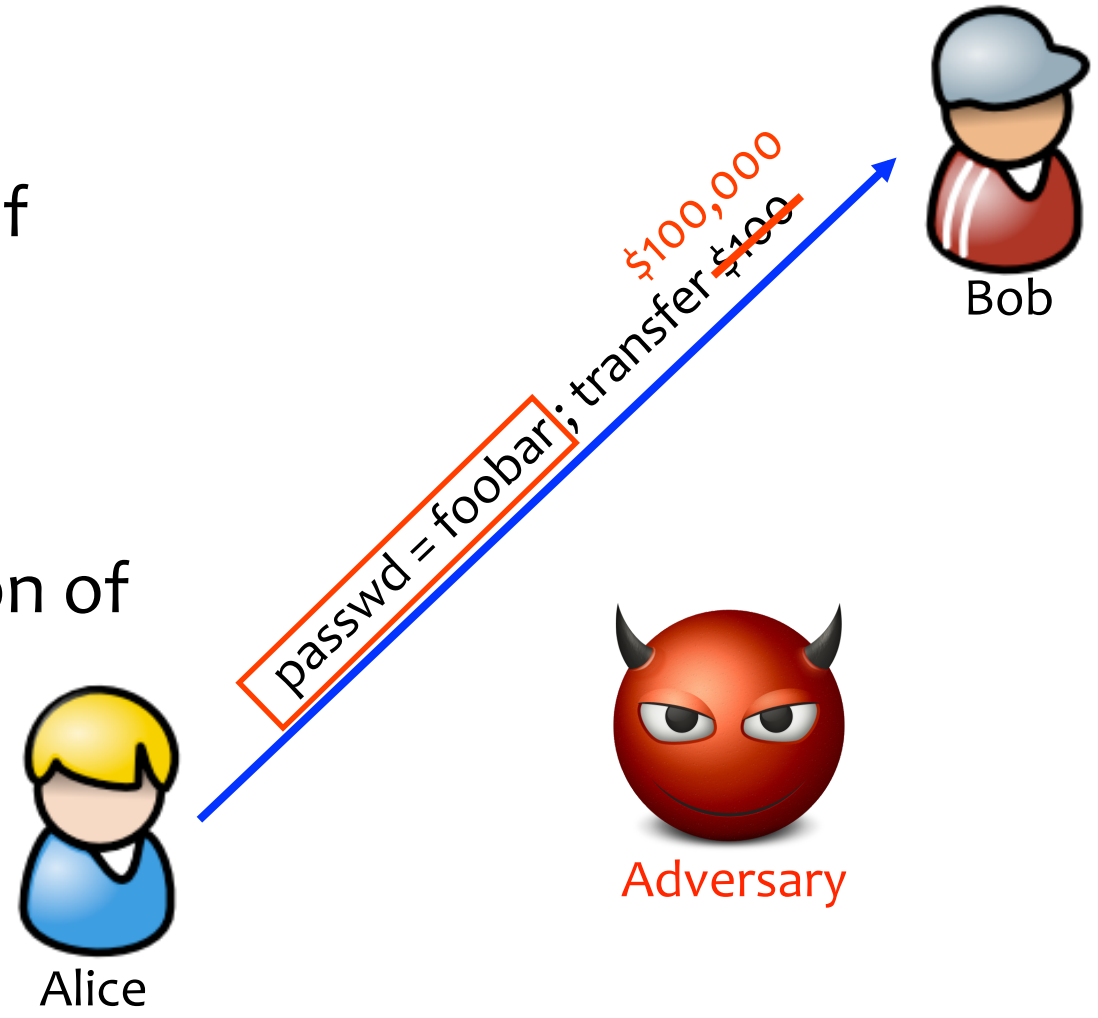
Common Communication Security Goals

Privacy of data:

Prevent exposure of information

Integrity of data:

Prevent modification of information



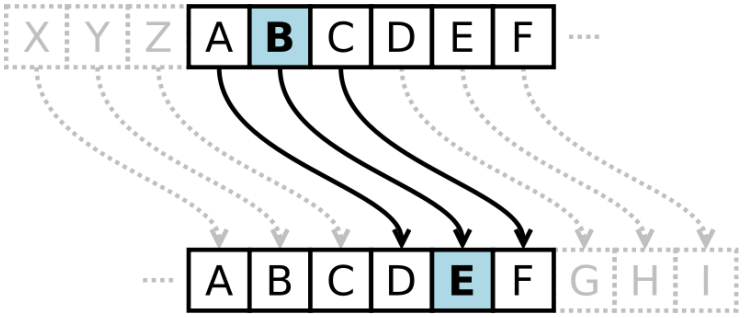
History

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

- Recommended Reading: **The Codebreakers** by David Kahn and **The Code Book** by Simon Singh.

History: Caesar Cipher (Shift Cipher)

- Plaintext letters are replaced with letters a fixed shift away in the alphabet.



- Example:
  - Plaintext: `The quick brown fox jumps over the lazy dog`
  - Key: Shift 3

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

  - Ciphertext: `WKHTX LFNEU RZQIR AMXPS VRYHU WKHOD CBGRJ`

History: Caesar Cipher (Shift Cipher)

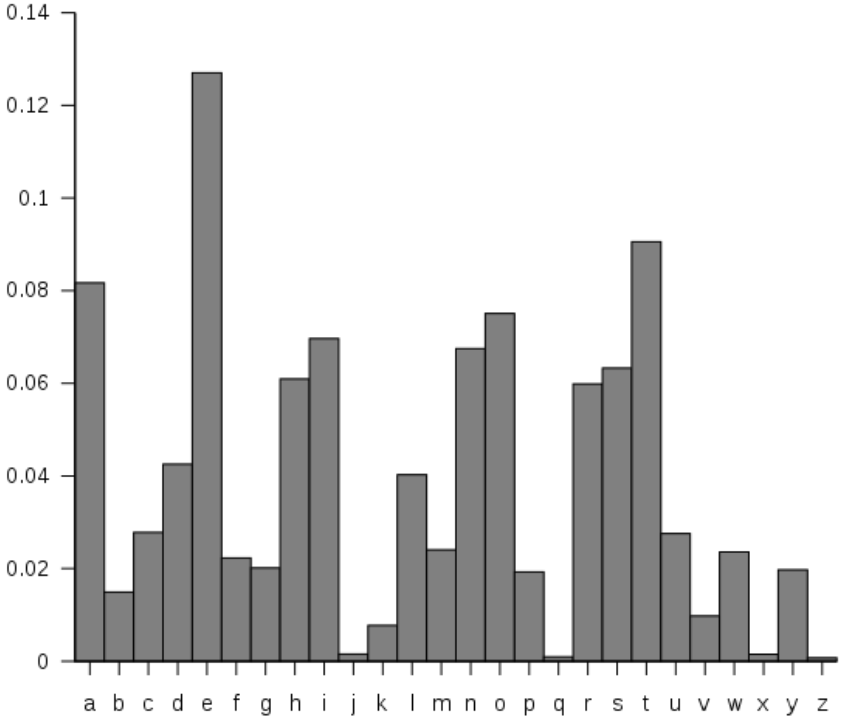
- ROT13: shift 13 (encryption and decryption are symmetric)
- What is the key space?
  - 26 possible shifts.
- How to attack shift ciphers?
  - Brute force.

History: Substitution Cipher

- Superset of shift ciphers: each letter is substituted for another one.
- Add a secret key
- Example:
  - Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Cipher: ZEBRASCDFGHIJKLMNOPQTUVWXY
- "State of the art" for thousands of years

History: Substitution Cipher

- What is the key space? 26! ~= 2^88
- How to attack?
  - Frequency analysis.



Bigrams:

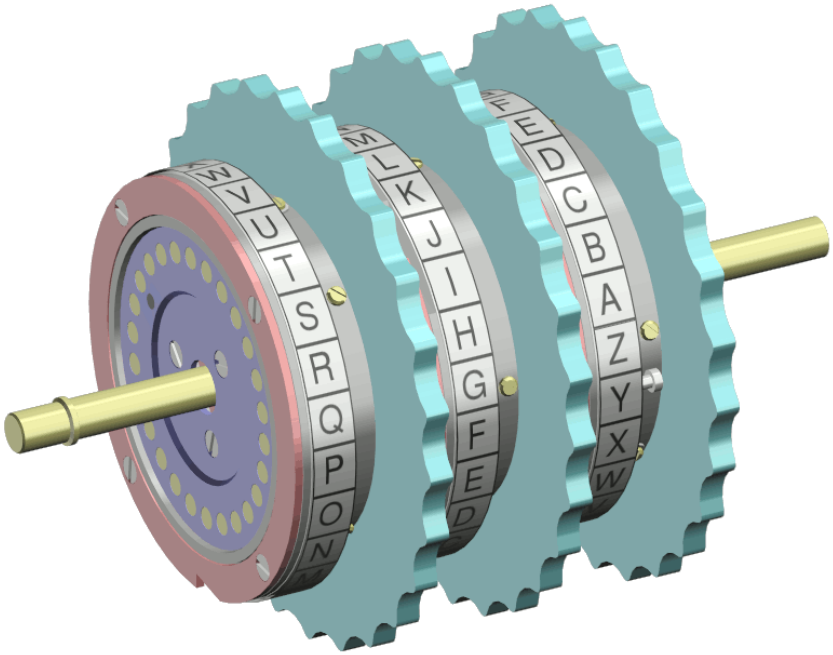
th 1.52%	en 0.55%	ng 0.18%
he 1.28%	ed 0.53%	of 0.16%
in 0.94%	to 0.52%	al 0.09%
er 0.94%	it 0.50%	de 0.09%
an 0.82%	ou 0.50%	se 0.08%
re 0.68%	ea 0.47%	le 0.08%
nd 0.63%	hi 0.46%	sa 0.06%
at 0.59%	is 0.46%	si 0.05%
on 0.57%	or 0.43%	ar 0.04%
nt 0.56%	ti 0.34%	ve 0.04%
ha 0.56%	as 0.33%	ra 0.04%
es 0.56%	te 0.27%	ld 0.02%
st 0.55%	et 0.19%	ur 0.02%

Trigrams:

1. the	6. ion	11. nce
2. and	7. tio	12. edt
3. tha	8. for	13. tis
4. ent	9. nde	14. oft
5. ing	10. has	15. sth

History: Enigma Machine

Uses rotors (substitution cipher) that change position after each key.



Key = initial setting of rotors

Key space?

26^n for n rotors

Kerckhoff's Principle

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

How Cryptosystems Work Today

- Layered approach:
  - Cryptographic primitives, like block ciphers, stream ciphers, hash functions, and one-way trapdoor permutations
  - 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)

- Don't roll your own!

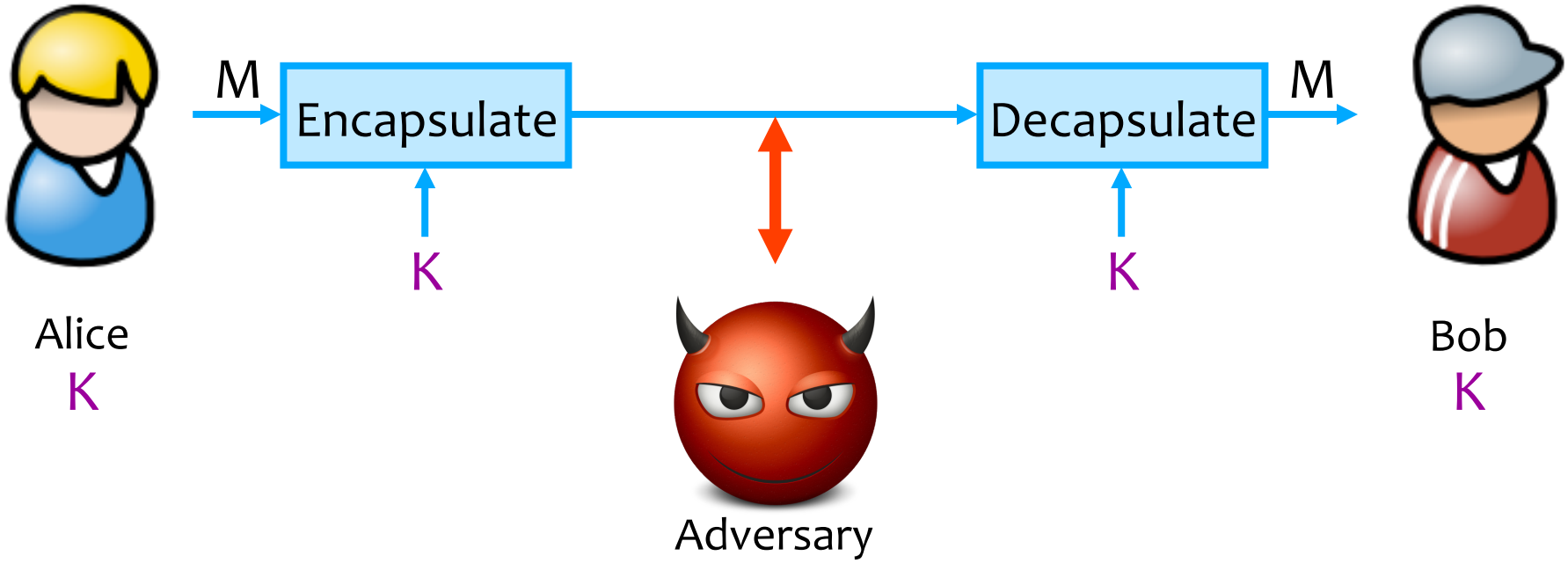
Flavors of Cryptography

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

- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.

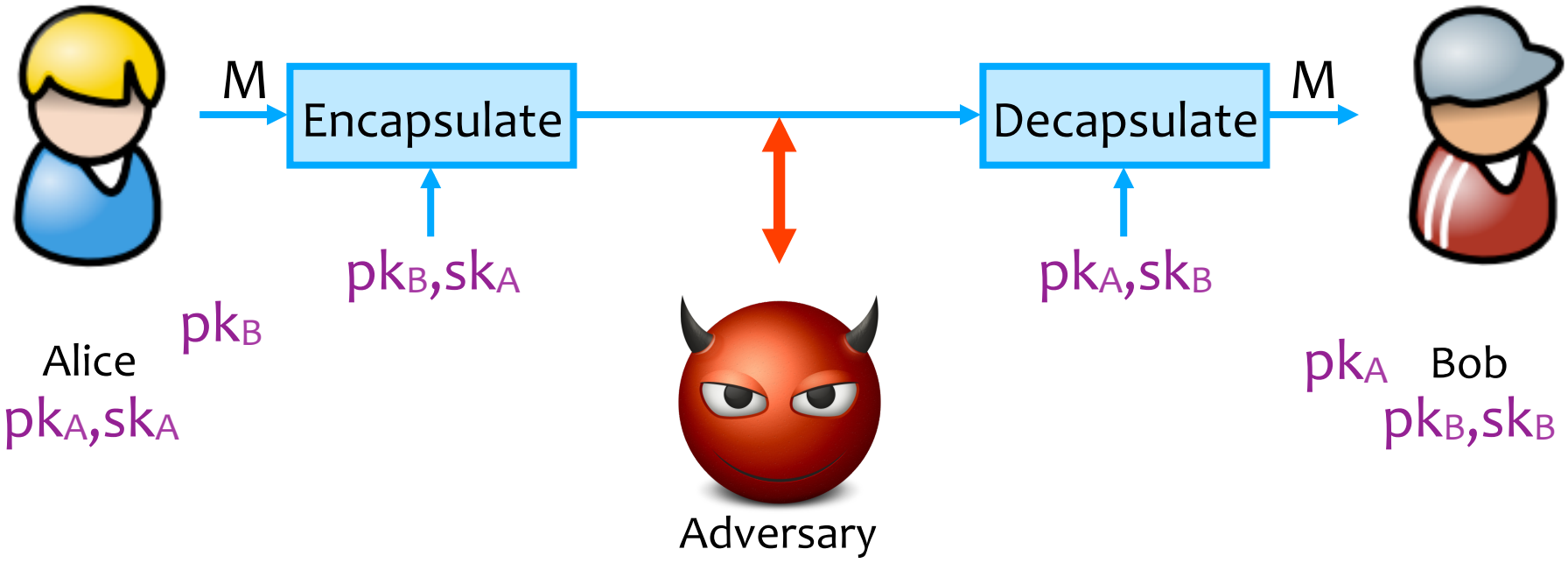
Symmetric Setting

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



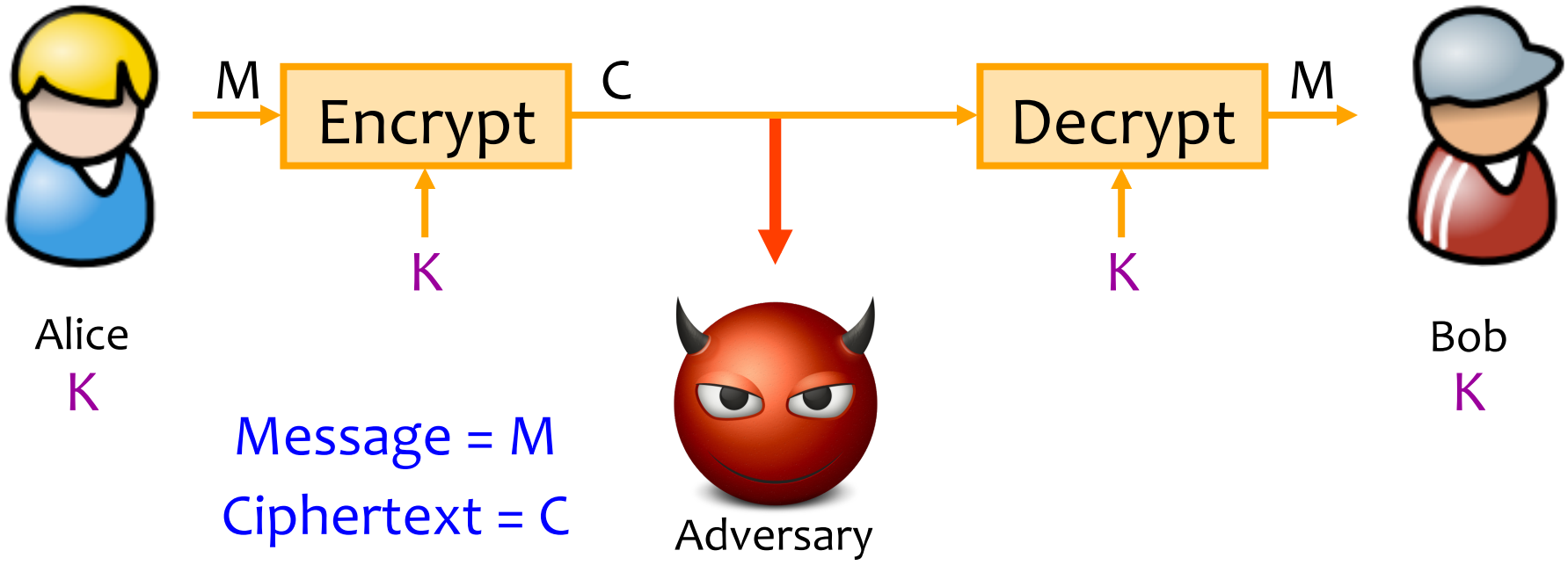
Asymmetric Setting

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



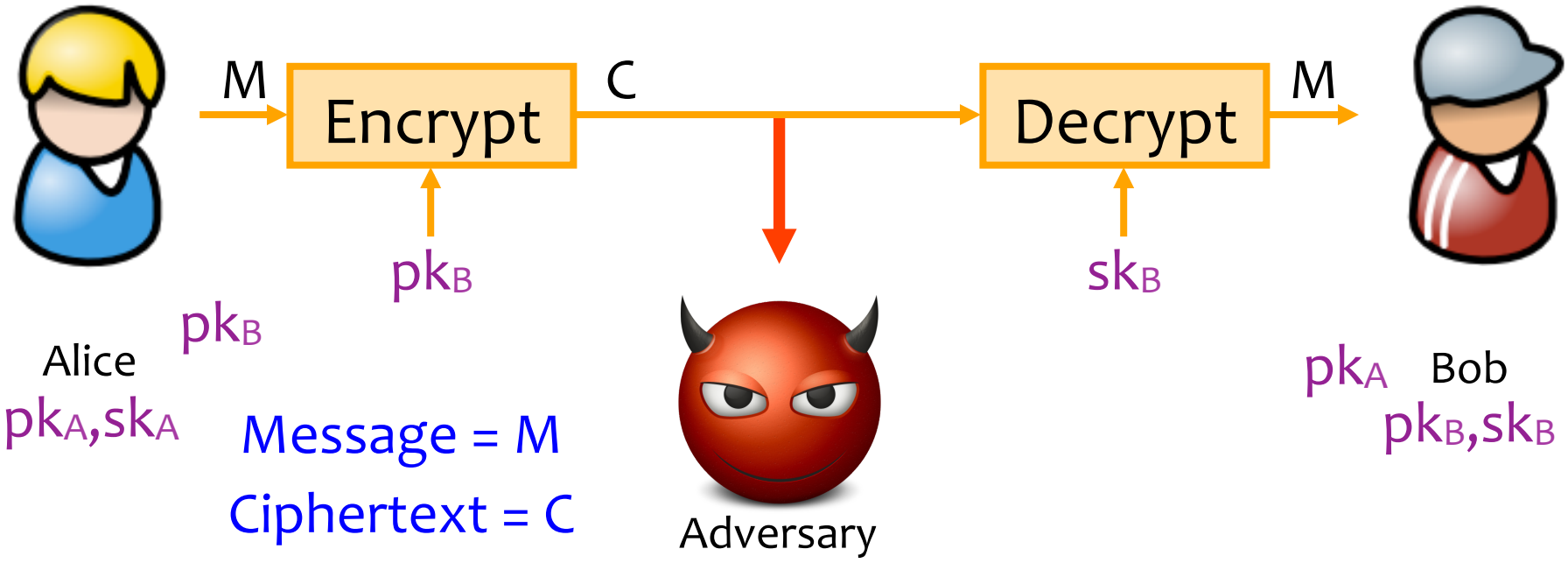
Achieving Privacy (Symmetric)

Encryption schemes: A tool for protecting privacy.



Achieving Privacy (Asymmetric)

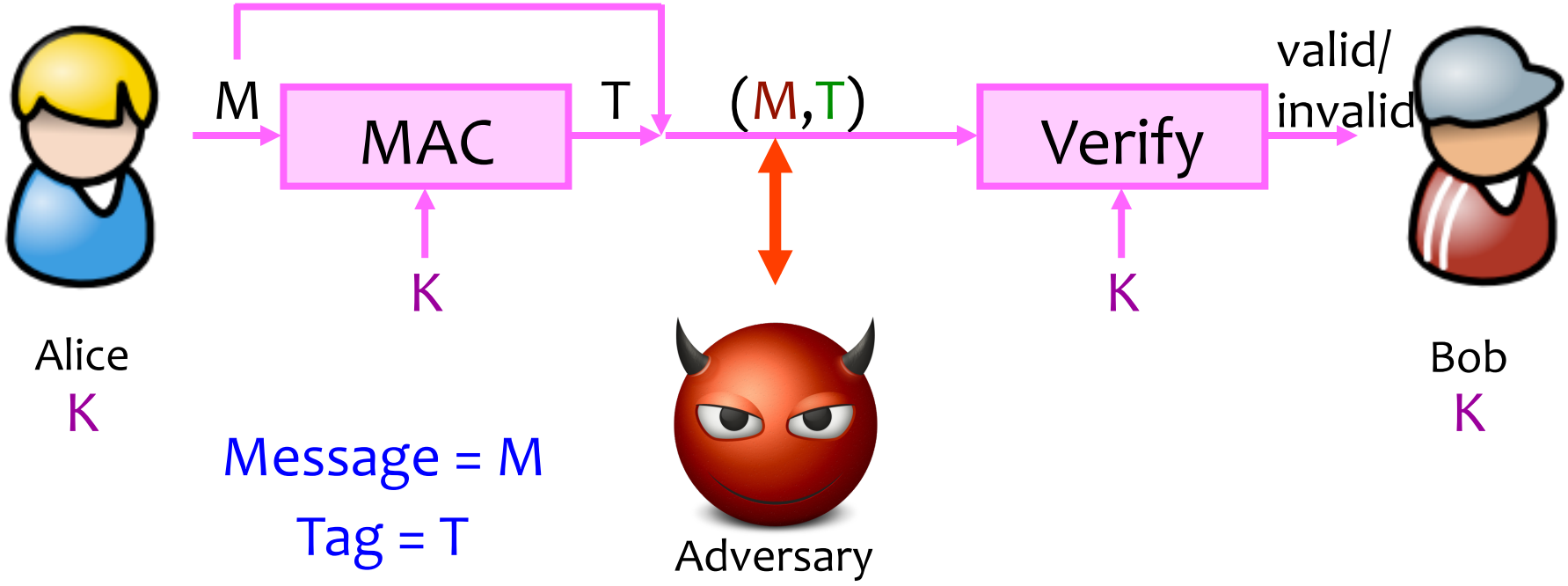
Encryption schemes: A tool for protecting privacy.



Achieving Integrity (Symmetric)

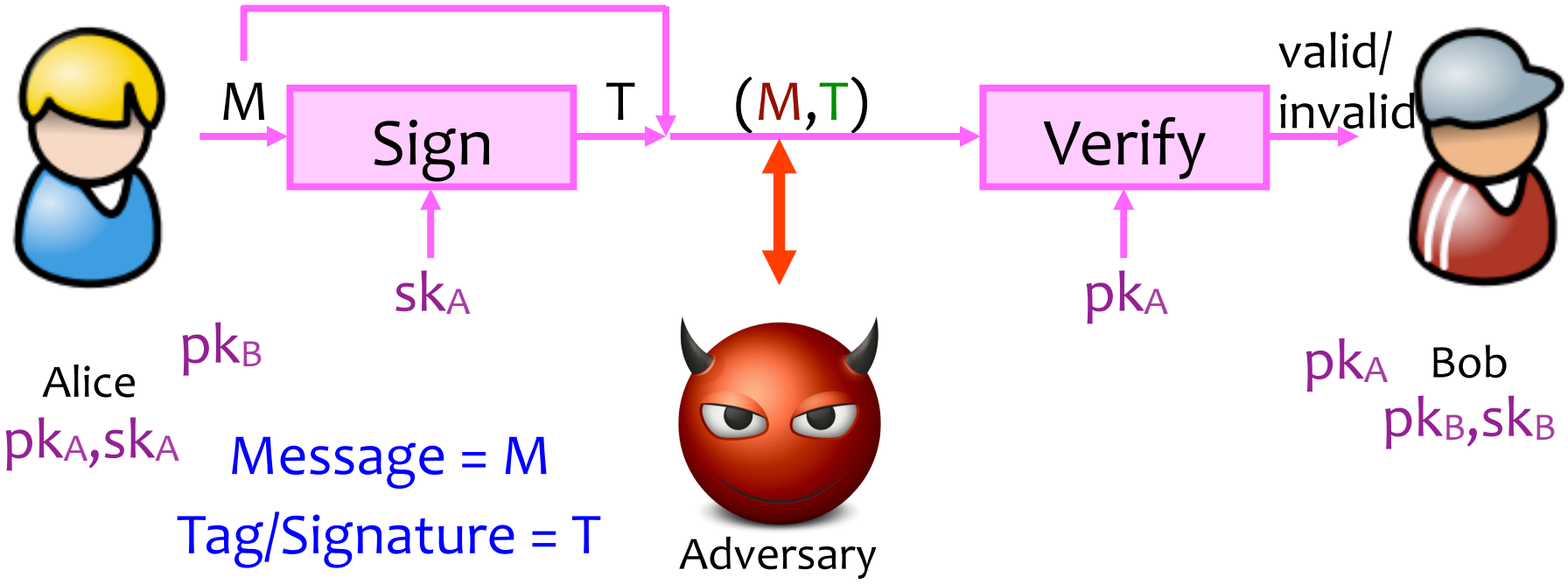
Message authentication schemes: A tool for protecting integrity.

(Also called message authentication codes or MACs.)



Achieving Integrity (Asymmetric)

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



Flavors of Cryptography

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

- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.

Flavors of Cryptography

- Symmetric cryptography
  - Both communicating parties have access to a shared random string K, called the key.
  - Challenge: How do you privately share a key?
- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.
  - Challenge: How do you validate a public key?