CAL POLY

CSC 321: Introduction to Computer Security

Module 3 Public Key Cryptography and Digital Signature

Bret Hartman

Department of Computer Science and Software Engineering

California Polytechnic State University

E-mail: bahartma@calpoly.edu

A special thanks to Dr. Bruce DeBruhl and Dr. Phoenix (Dongfeng) Fang, the authors of most of this material

Quiz 2 available
Assignment 2 Block Ciphers due

The problem of key distribution

- Any thoughts on how keys can be distributed?
- Traditionally key distribution centers were used

What good would it do after all to develop impenetrable cryptosystems, if their users were forced to share their keys with a KDC that could be compromised by either burglary or subpoena.

Whitfield Diffie, 1988

The rise and fall of RSA

1976

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN,

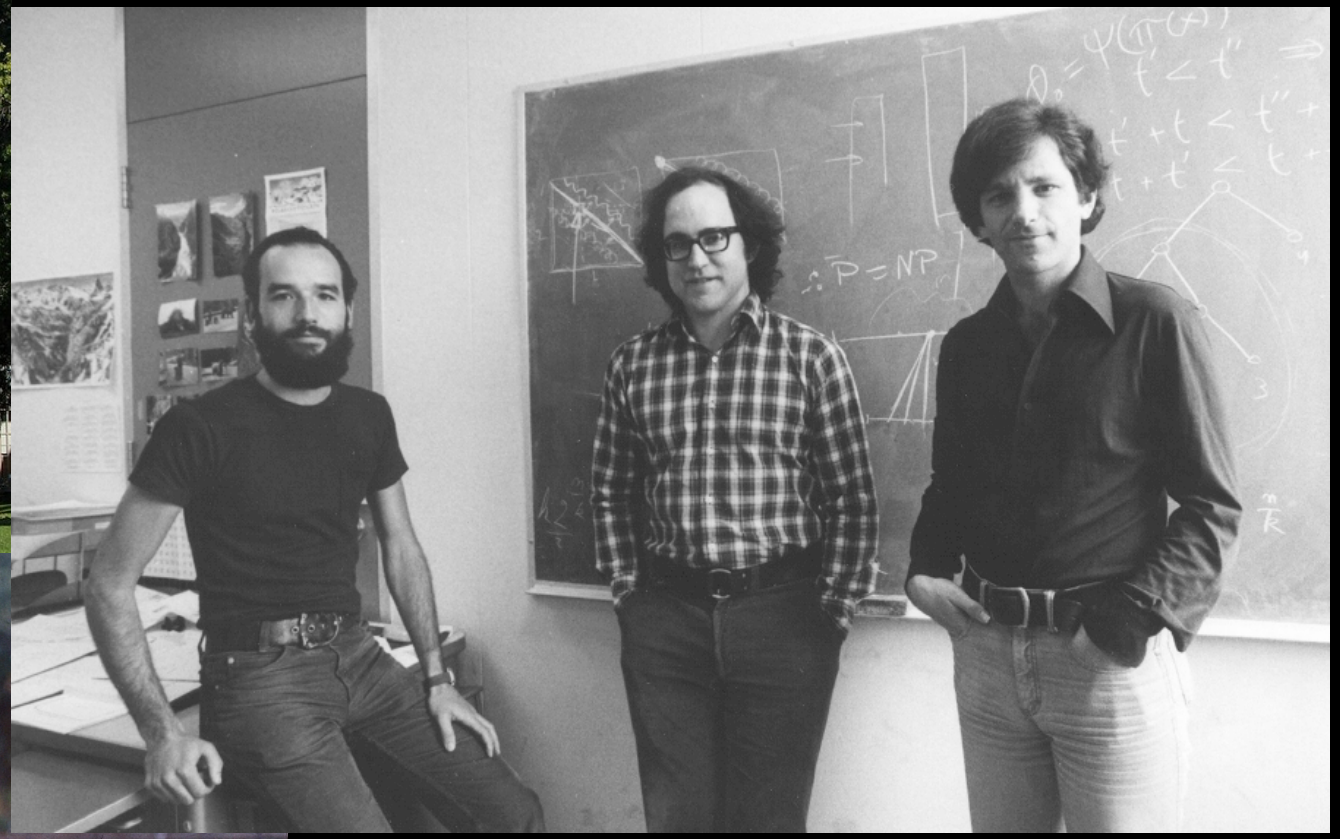
Abstract—**Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

The best known
vacy: preventing th
tion from communi
order to use cryptog
currently necessary
a key which is know
ing the key in adva
private courier or re

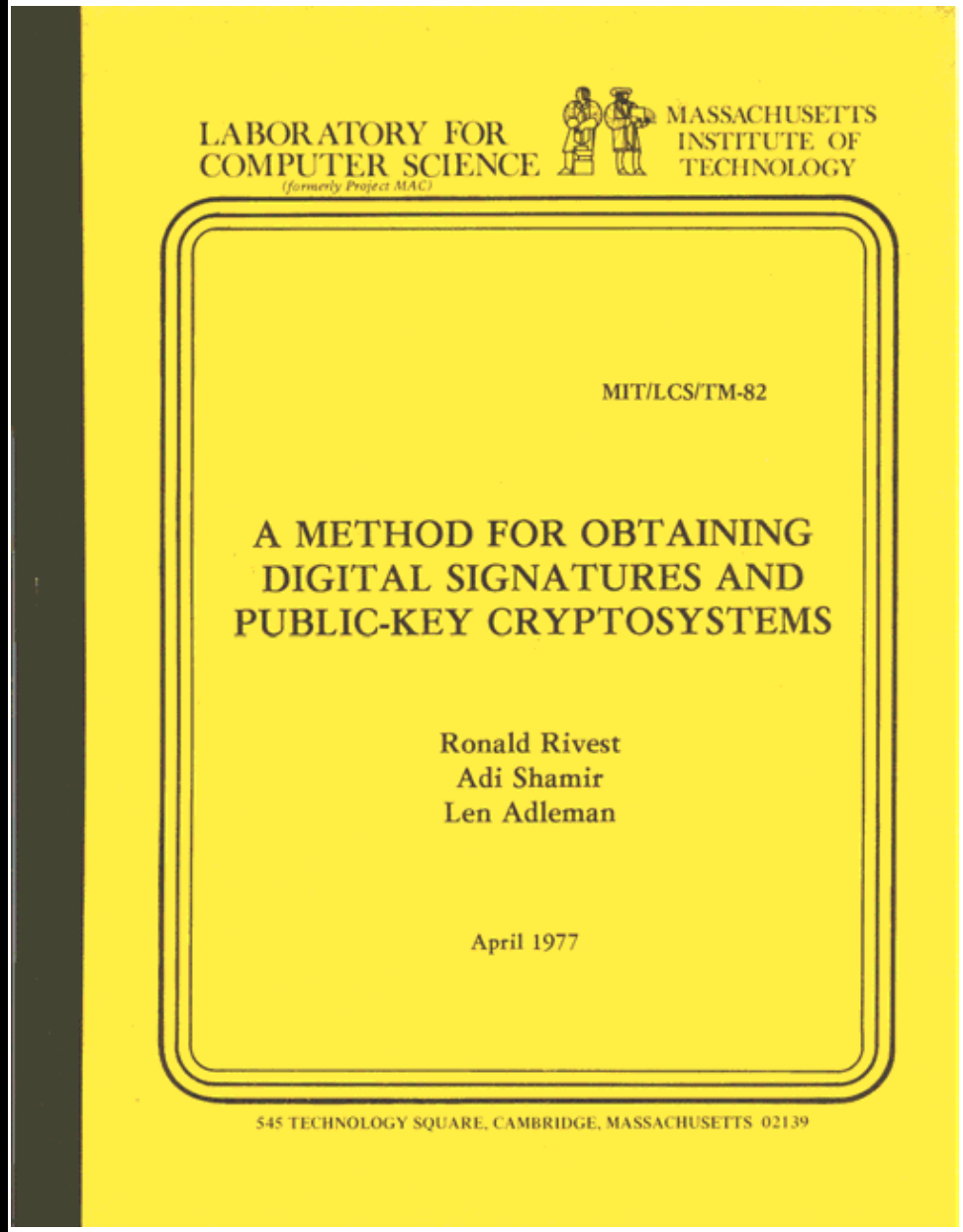
I. Introduction

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

1976



1977



LABORATORY FOR COMPUTER SCIENCE
(formerly Project MAC)

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MIT/LCS/TM-82

A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS

Ronald Rivest
Adi Shamir
Len Adleman

April 1977

545 TECHNOLOGY SQUARE, CAMBRIDGE, MASSACHUSETTS 02139

Programming Techniques
S.L. Graham, R.L. Rivest*
Editors

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R. L. Rivest, A. Shamir, and L. Adleman
MIT Laboratory for Computer Science
and Department of Mathematics

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:
(1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
(2) A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems. A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, *n*, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e * d = 1 (\mathrm{mod}\ (p-1) * (q-1))$. The security of the system rests in part on the difficulty of factoring the published divisor, *n*.

Key Words and Phrases: digital signatures, public-key cryptosystems, privacy, authentication, security, factorization, prime number, electronic mail, message-passing, electronic funds transfer, cryptography.
CR Categories: 2.12, 3.15, 3.50, 3.81, 5.25

This research was supported by National Science Foundation grant MCS76-14294, and the Office of Naval Research grant number N00014-67-A-0204-0063.

* Note. This paper was submitted prior to the time that Rivest became editor of the department, and editorial consideration was completed under the former editor, G. K. Manacher.

Authors' Address: MIT Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139.

I. Introduction

The era of "electronic mail" [10] may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system.

At the heart of our proposal is a new encryption method. This method provides an implementation of a "public-key cryptosystem", an elegant concept invented by Diffie and Hellman [1]. Their article motivated our research, since they presented the concept but not any practical implementation of such a system. Readers familiar with [1] may wish to skip directly to Section V for a description of our method.

II. Public-Key Cryptosystems

In a "public-key cryptosystem" each user places in a public file an encryption procedure E. That is, the public file is a directory giving the encryption procedure of each user. The user keeps secret the details of his corresponding decryption procedure D. These procedures have the following four properties:

(a) Deciphering the enciphered form of a message M yields M. Formally,

$$D(E(M)) = M. \quad (1)$$

(b) Both E and D are easy to compute.

(c) By publicly revealing E the user does not reveal an easy way to compute D. This means that in practice only he can decrypt messages encrypted with E, or compute D efficiently.

(d) If a message M is first deciphered and then enciphered, M is the result. Formally,

$$E(D(M)) = M. \quad (2)$$

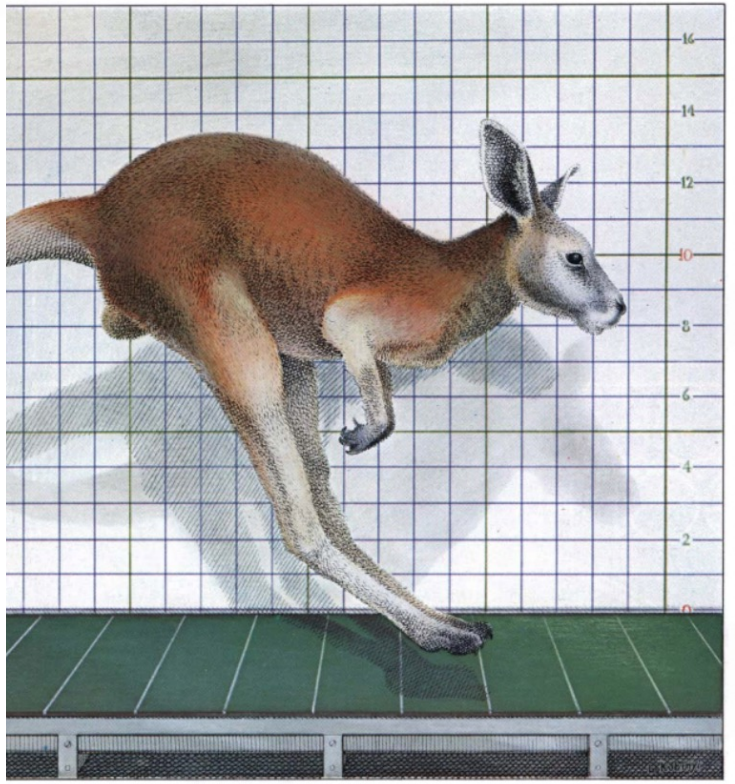
An encryption (or decryption) procedure typically consists of a *general method* and an *encryption key*. The general method, under control of the key, enciphers a message M to obtain the enciphered form of the message, called the *ciphertext* C. Everyone can use the same general method; the security of a given procedure will rest on the security of the key. Revealing an encryption algorithm then means revealing the key.

When the user reveals E he reveals a very *inefficient* method of computing D(C): testing all possible messages M until one such that E(M) = C is found. If property (c) is satisfied the number of such messages to test will be so large that this approach is impractical.

A function E satisfying (a)-(c) is a "trap-door one-way function;" if it also satisfies (d) it is a "trap-door one-way permutation." Diffie and Hellman [1] introduced the concept of trap-door one-way functions but

1977

SCIENTIFIC AMERICAN



KANGAROOS

$1.50

August 1977

MATHEMATICAL GAMES

A new kind of cipher that would take millions of years to break

by Martin Gardner

"Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."

—EDGAR ALLAN POE

The upward creep of postal rates accompanied by the deterioration of postal service is a trend that may or may not continue, but as far as most private communication is concerned, in a few decades it probably will not matter. The reason is simple. The transfer of information will probably be much faster and much cheaper by "electronic mail" than by conventional postal systems. Before long it should be possible to go to any telephone, insert a message into an attachment and dial a number. The telephone at the other end will print out the message at once.

is unbreakable by sophisticated cryptanalysis? The surprising answer is yes. The breakthrough is scarcely two years old, yet it bids fair to revolutionize the entire field of secret communication. Indeed, it is so revolutionary that all previous ciphers, together with the techniques for cracking them, may soon fade into oblivion.

An unbreakable code can be unbreakable in theory or unbreakable only in practice. Edgar Allan Poe, who fancied himself a skilled cryptanalyst, was convinced that no cipher could be invented that could not also be "unriddled." Poe was certainly wrong. Ciphers that are unbreakable even in theory have been in use for half a century. They are "one-time pads," ciphers that are used only once, for a single message. Here is a simple example based on a shift cipher, sometimes called a Caesar cipher because Julius Caesar used it.

First write the alphabet, followed by

encoded, the arrow is spun and the lower sequence is shifted accordingly. The result is a ciphertext starting with J and a cipher "key" starting with K. Note that the cipher key will be the same length as the plaintext.

To use this one-time cipher for sending a message to someone—call him *Z*—we must first send *Z* the key. This can be done by a trusted courier. Later we send to *Z*,
decodes it with the key and then destroys the key. The key must not be used again because if two such ciphertexts were intercepted, a cryptanalyst might have sufficient structure for breaking them.

It is easy to see why the one-time cipher is uncrackable even in principle. Since each symbol can be represented by any other symbol, and each choice of representation is completely random, there is no internal pattern. To put it another way, any message whatever having the same length as the ciphertext is as legitimate a decoding as any other. Even if the plaintext of such a coded message is found, it is of no future help to the cryptanalyst because the next time the system is used the randomly chosen key will be entirely different.

One-time pads are in constant use today for special messages between high military commanders, and between governments and their high-ranking agents. The "pad" is no more than a long list of random numbers, perhaps printed on many pages. The sender and receiver must of course have duplicate copies. The sender uses page 1 for a cipher, then destroys the page. The receiver uses his page 1 for decoding, then destroys his page. When the Russian agent Rudolf

1983

United States Patent [19]

Rivest et al.

[11] **4,405,829**

[45] **Sep. 20, 1983**

[54] **CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD**

[75] Inventors: **Ronald L. Rivest**, Belmont; **Adi Shamir**, Cambridge; **Leonard M. Adleman**, Arlington, all of Mass.

[73] Assignee: **Massachusetts Institute of Technology**, Cambridge, Mass.

[21] Appl. No.: **860,586**

[22] Filed: **Dec. 14, 1977**

Primary Examiner—Sal Cangialosi
Attorney, Agent, or Firm—Arthur A. Smith, Jr.; Robert J. Horn, Jr.

[57] **ABSTRACT**

A cryptographic communications system and method. The system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. A message-to-be-transferred is enciphered to ciphertext at the encoding terminal by first encoding the message as

1983-1986


DON'T COMMUNICATE, DEDICATE!
DEDICATE/32™
for Positive
Data Security
FRED, DON'T RELEASE THAT
COULD DO DAMAGE TO.
FURTHER RESEARCH NEEDED
SIGNED, JOHN DOE, PRES.
NAIFMOEBMOCHIBEKN
OOTBCDELMBNAAOJB
JHIPECMNOCPNABGI
FNECNOJBPEMDDAE
INTRODUCTORY
PRICE $225
Quantity Discounts
Dealers Welcome
RSA Public Key encryption is available. With a modulus size of 77 digits. And Electronic Signatures. Really! And it's Fast! And easy!
Discover what Convenience and Positive Data Security really mean. Today. Because we have it — today.
Due to export controls, not available outside U.S. & Canada.
PKS
PUBLIC KEY SYSTEMS CORP.
P.O. Box 1130, Fayetteville, AR 72702 • (501) 442-0914


PC MAGAZINE
THE SHOWCASE FOR PRODUCTS AND SERVICES IN THE MS DOS MARKET . . .
MARKETPLACE
MAILSAFE™
A software implementation of the RSA public key cryptosystem for MS-DOS.
• Secure Messaging without secret sharing
• User key generation
• RSA Digital Signature ™ User file authentication
• RSA Digital Envelope ™ secure data privacy
• Local file encryption
• Configuration features for most E MAIL Systems
• OEM versions available for DOS and UNIX
$250 per copy Quantity discounts Special prices for government and education markets
The RSA public key crypto system is protected by US patent 4,405,829
CALL FOR INTRODUCTORY OFFER.
RSA DATA SECURITY, INC.
10 Twin Dolphin Drive • Redwood City, CA 94065
415/595-8782
CIRCLE 786 ON READER SERVICE CARD

1986-1991

Lotus contract with RSA Data Security in works

By Peggy Watt

CAMBRIDGE, Mass. — Lotus Development Corp. is expected this week to announce that it has licensed RSA Data Security, Inc. of San Carlos, Calif., to develop an encryption system for a new Lotus product.

Lotus and RSA would not disclose details of the system, but RSA specializes in dat… tra… has… me… par… tio… file… enc… me… I… con… T… fication features, she …. The spokeswoman said contract is a multiyear …ement and may eventual…nvolve more than one Lo… product. …SA's encryption method …tes a digital seal, or sig…re code, that can be de…oted by a public key, or …ry numerical password.

IBM prod…

From page 23

from $30 t… If a PC … IBM warr… maintenanc… of its add-… der origina… be included… tenance ag… For cust… pair, the m…

JUNE 10, 1991

Microsoft Licenses RSA Data Encryption Security Technology

BY BARBARA DARROW

Microsoft is joining other industry powers in pledging allegiance to data encryption technology developed by RSA Data Security Inc.

By licensing RSA's Bsafe and Tipem cryptographic toolkits last week, Microsoft will be able to better safeguard sensitive electronic documents from unauthorized personnel, analysts said.

RSA Data Security's E-mail security pack draws raves

Innovative encryption software detects viruses.

By Barton Crockett
Senior Editor

REDWOOD CITY, Calif. — Data encryption software sold by a small company here is wooing a growing number of devotees who claim the technology offers a unique way to secure electronic mail and EDI messages.

Some users also said the software provides an effective way to detect viruses and software bugs.

RSA Data Security, Inc.'s Public Key Cryptosystem uses a proprietary system of public and private "keys" to scramble messages. The technology can also be used to create electronic "signatures" that show if messages have been tampered with.

Among users of the RSA Data Security technology is Internet, the network that connects academic, government and industry networks across the country. Internet, which was ravaged by a hacker last year, announced early this spring that it would use the RSA Data Security public/private key and signature technology in a new secure E-mail system it is developing.

The RSA Data Security encryption technology is based on an algorithm patented in the late 1970s by Massachusetts Institute of Technology professors Ronald Rivest, Adi Shamir and Len Adleman. It is licensed exclusively by RSA Data Security, which was founded by the three professors in 1982.

What distinguishes the RSA Data Security technology from other encryption systems is the way it pairs public and private keys. A file that is encrypted using an RSA Data Security public key can only be decrypted using the matching private key, and vice versa.

This allows a user to encrypt an E-mail message using the published public key of the addressee. Only the addressee, who has sole access to his private key, can decrypt the message.

"For what we need, RSA is the only game in town," said Stephen Kent, chief scientist at BBN Communications Corp. in Cambridge, Mass., and chairman of the Internet privacy task force that is de-

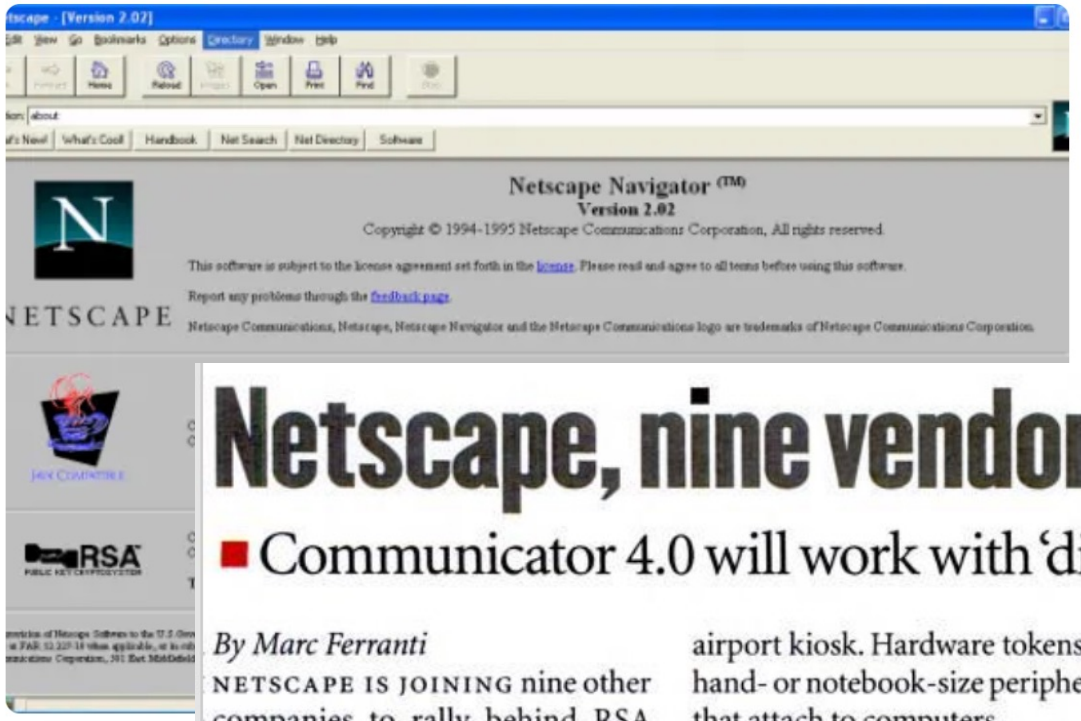
(continued on page 48)

1995

This Day In Market History: The Netscape IPO

Wayne Duggan

August 9, 2018



The Origins of Web Security and the Birth of Security Socket Layer (SSL) Protocol

Netscape, nine vendors to back RSA standard

Communicator 4.0 will work with 'digital certificates' for access to Web sites

By Marc Ferranti

NETSCAPE IS JOINING nine other companies to rally behind RSA Data Security's cryptography standard for smart cards and hardware tokens, the company announced last week.

airport kiosk. Hardware tokens are hand- or notebook-size peripherals that attach to computers.

Netscape also announced that its recently launched Communicator 4.0 Internet communications package works with "digital certificates"

Netscape officials likened digital certificates to a digital driver's license, which users can present on the Internet when accessing e-mail or data on corporate networks. Certificates are designed to deliver a stronger form of authentication

committed to supporting RSA's Public Key Cryptography Standard, or PKCS #11, for smart cards and tokens and are incorporating the standard into interoperable solutions for enhanced protection of corporate data.

1995

Here Is the First Book Ever Ordered on Amazon

By Megan Garber

OCTOBER 31, 2012

... and the packing slip that c

RSA's Precocious Spinoff Making a Name in Internet Security

April 15, 1996, 1:00 a.m. EDT 3 Min Read

Were it not for the fact that its staff is bigger than that of its corporate forebear, Verisign Inc. might be called mini-RSA.

Spun off 12 months ago by RSA Data Security Inc., Verisign has similarly established its credentials throughout the electronic commerce realm. It aims, according to president Stratton Sclavos, "to be to digital authentication what RSA is to data encryption."

2000

Clock ticking on key encryption patent

Change could mean lower prices for security products using RSA public-key technology.

BY ELLEN MESSMER

SAN JOSE — RSA Security's patent for the most important encryption technology used in corporate networks is set to expire in September — an event that could lead to lower prices for software incorporating RSA public-key technology and new challenges to RSA Security's encryption industry leadership.

use the patented technology. Jim Bidzos, once the company president and now vice chairman of RSA Security's board of directors, built up the company's business through licensing deals.

But with its key patent expiring on Sept. 21, RSA Security for the first time is bound to find competitors. Chief among these firms will

week hosted about 8,000 people at its annual security conference in San Jose, wasn't willing to discuss its licensing policies in detail.

RSA Security does acknowledge its tool kits still account for about 30% of its revenue, but says it's not worried about the impending loss of its patent. The company has some large and apparently content

still go to RSA."

But there are a couple of other possible ramifications of

FEATURE

RSA encryption patent released

Algorithm can now be used free of charge

By Ann Harrison

Computerworld | SEP 18, 2000 12:00 AM PST

SAN FRANCISCO

RSA Security Inc. pre-empted a number of celebration parties by unexpectedly releasing the widely used RSA public-key encryption algorithm into the public domain ahead of this week's expiration of the patent on the algorithm.

2006-2010

NEWS

Update: EMC to acquire RSA Security for almost $2.1B

The companies hope to position themselves more effectively in the data security market

Symantec Acquires VeriSign for $1.28 Billion

BY DEALBOOK AUGUST 10, 2010 6:41 AM Comment

Symantec has completed its $1.28 billion purchase of the Web-authentification business of VeriSign, The Silicon Valley Mercury News reported.

Symantec, which makes security and data-storage software, will acquire VeriSign's Secure Sockets Layer technology, which is used by businesses likebanks and retailers to ensure that their Web sites are safe for consumers to use.

2015-2021

TLS 1.3 Working Group Has Consensus to Deprecate RSA Key Transport

Author:
Michael Mimos
May 6, 2014 / 1:11
2 minute read
Share this article:

May 6, 2021, 07:40am EDT | 2,228 views

RSA Is Dead — We Just

COMPUTING

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

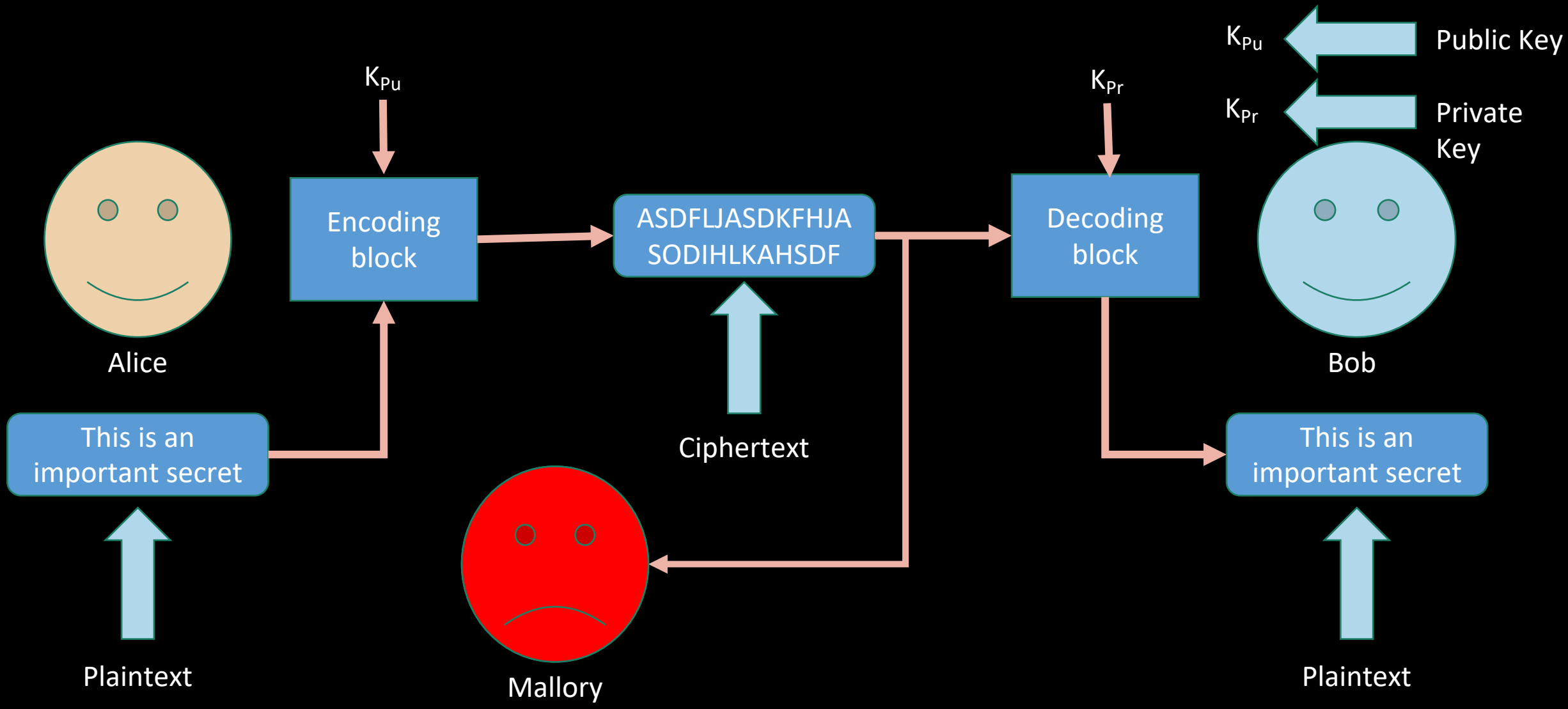
By Emerging Technology from the arXiv

May 30, 2019

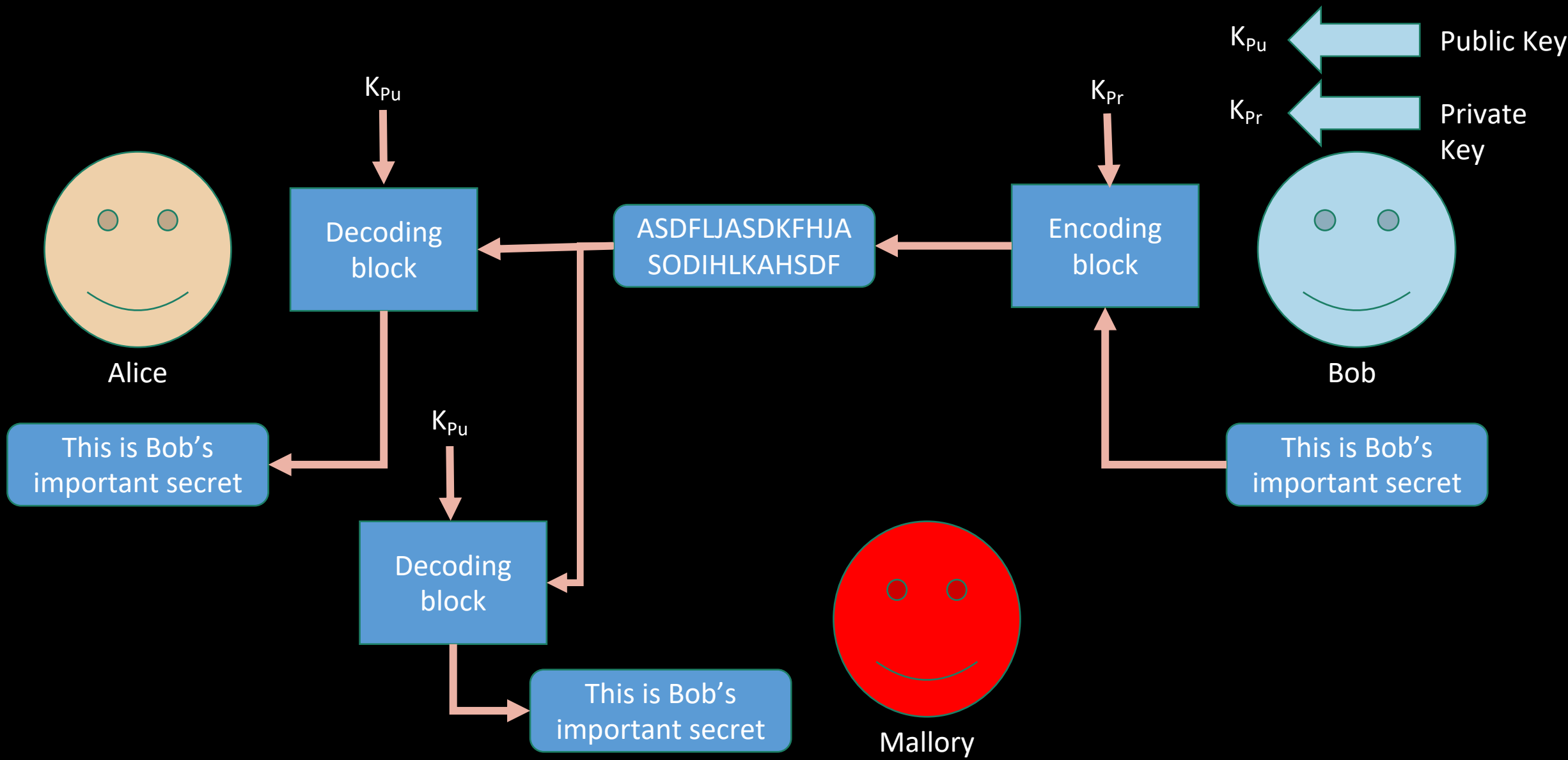
RSA

pen source
it all. But one
me inexplicable
m to use. Let me
save you a bit of time and money and just say outright—if you come to us
with a codebase that uses RSA, you will be paying for the hour of time

Public key crypto - encryption

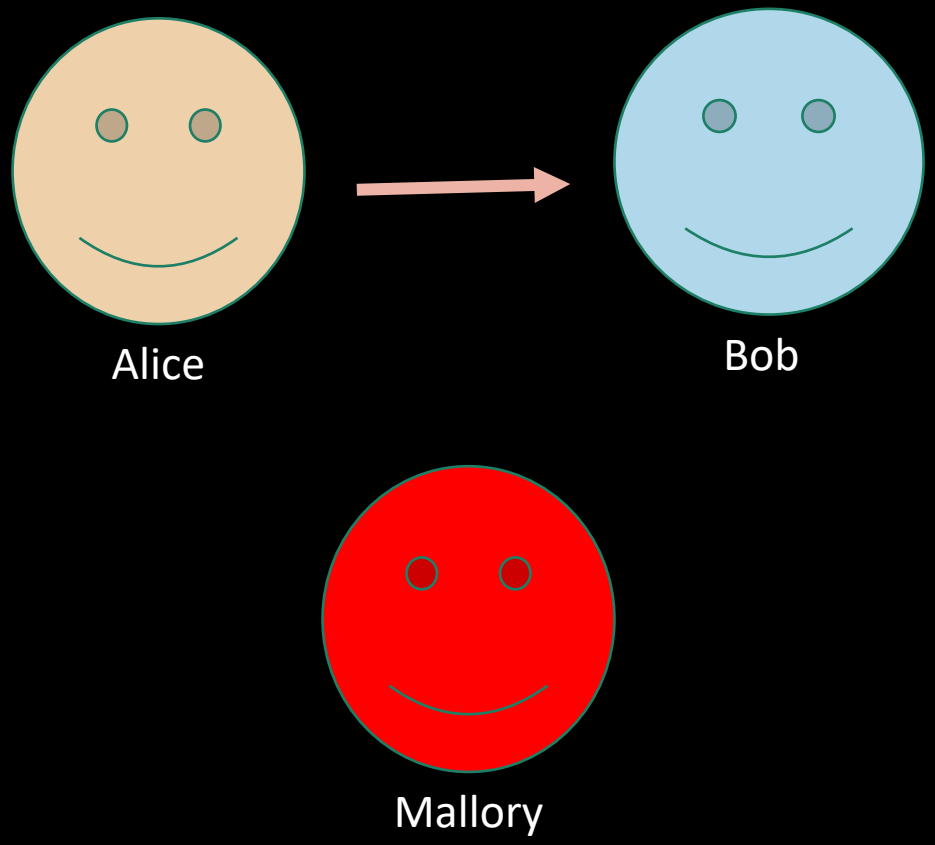


Public key crypto – digital signature



Quick questions

- For encryption who has the public key?
- What is the public key used for?
- For encryption who has the private key?
- What is the private key used for?
- For signing who has the public key?
- What is the private key used for?



Important public-key algorithms

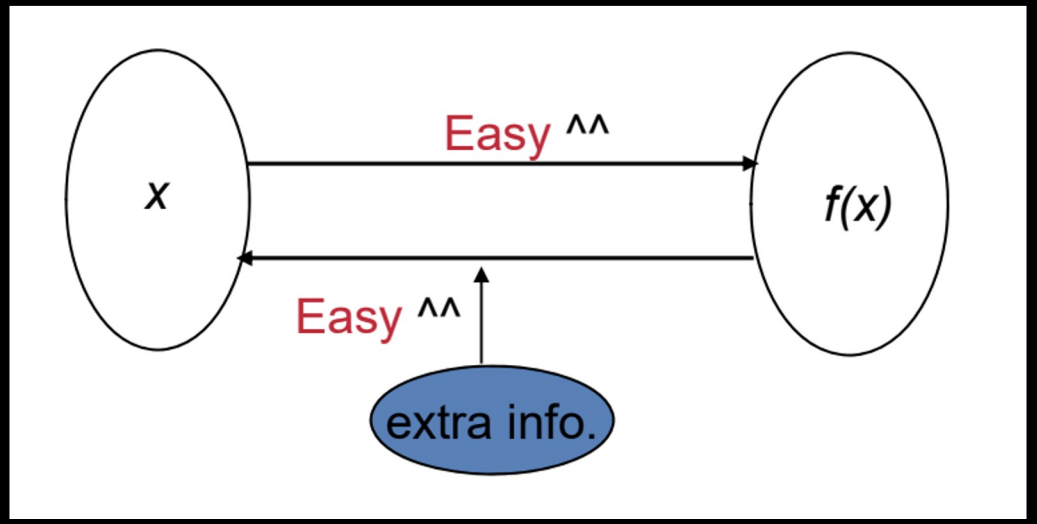
- Diffie Hellman Key Exchange
- RSA (Rivest, Shamir, Adleman)
- Elliptic curve
- El Gamal
- DSS (Digital Signature Standard)

This class focuses on the first two

Diffie-Hellman key exchange

- Named after Whitfield Diffie and Martin Hellman of Stanford in 1976
- Key length: variable bit size (1024, 2048, 4096, and larger)
- Based on difficulty of computing discrete logarithms
- Applications
  - Key exchange only
  - For session symmetric key establishment
  - Can be used when Alice and Bob have never met and share no secrets

Public-key cryptography requires trap-door one-way function



Recalling modular math

- Imagine math on a clock
  - For a mod 12 arithmetic
    - 13 mod 12 = 1
    - 8 mod 12 = 8
    - 52 mod 12 = ?
      - 4
    - -11 mod 12 = ?
      - 1

Discrete logarithms

- Assume
  - Order n
  - Generator α
- The discrete log x of β to the base α is
  - Given β, α
  - Find x s.t. $\beta = \alpha^x \bmod n$
  - This is hard

Diffie-Hellman protocol

Global Public Elements	
q	Prime number
α	$\alpha < q$ and α a primitive root of q

User A Key Generation	
Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

User B Key Generation	
Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$

Generation of Secret Key by User A
$K = (Y_B)^{X_A} \bmod q$

Generation of Secret Key by User B
$K = (Y_A)^{X_B} \bmod q$

- q = 23
- α = 5

α is a primitive root of q: $\alpha^1 \bmod q$, $\alpha^2 \bmod q$, $\alpha^3 \bmod q$, … are permutations of the integers from 1 though q-1

- $X_A = 6$
- $Y_A = 5^6 \bmod 23 = 8$

$X_A, X_B \in \mathbb{Z}_q$, the integers relatively prime to q

- $X_B = 15$
- $Y_B = 5^{15} \bmod 23 = 19$

- $K = 19^6 \bmod 23 = 2$

- $K = 8^{15} \bmod 23 = 2$

Eve's brute force attack to find shared secret key

Global public elements
- Prime: q = 23
- Primitive root: α = 5

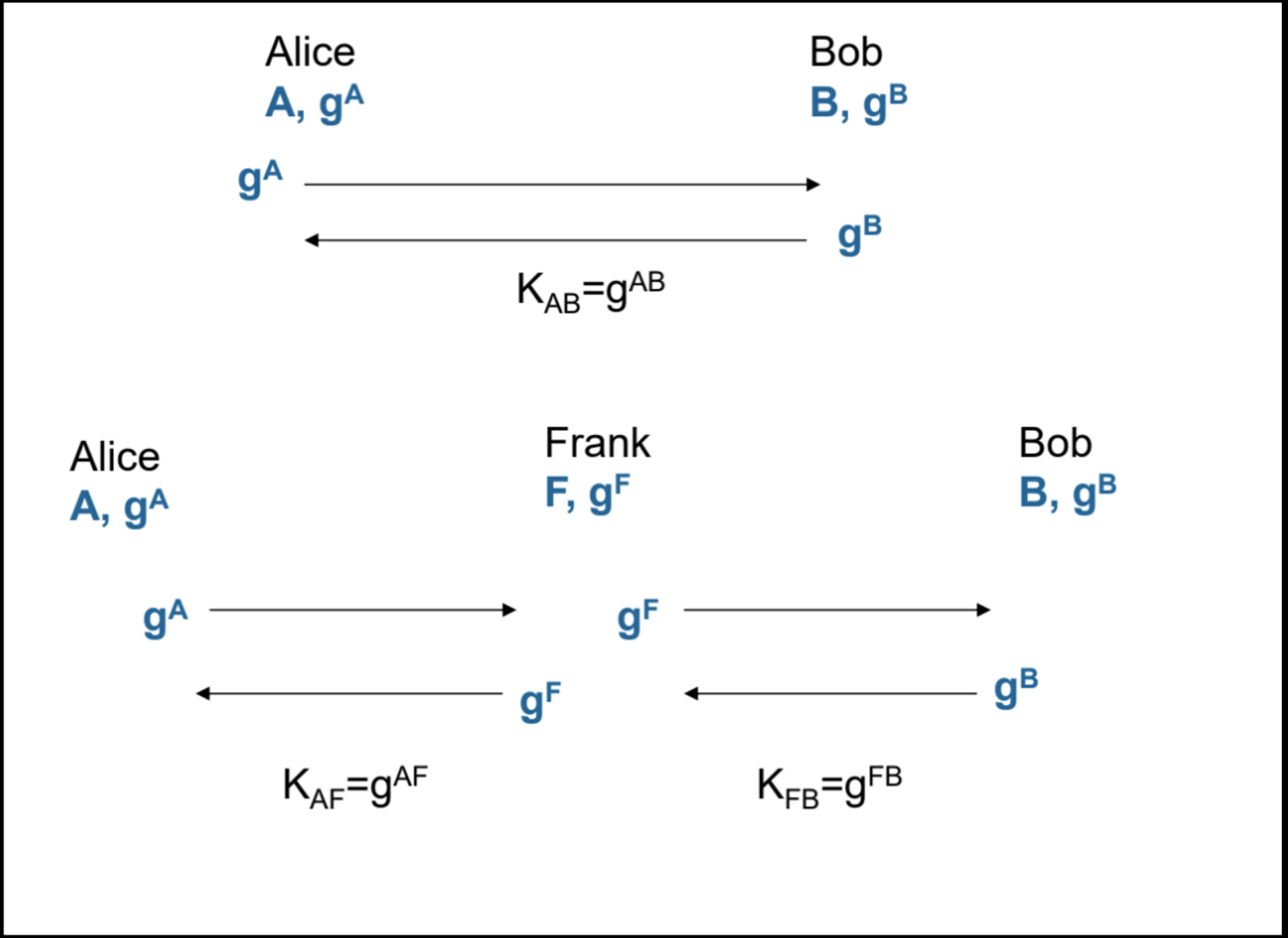
Alice's private/public key
- $X_A = 6$
- $Y_A = 5^6 \bmod 23 = 8$

Bob's public key
- $Y_B = 19$

Generation of shared secret K by Alice
- $K = 19^6 \bmod 23 = 2$

- Knowing q and α, Eve needs to find Alice's private key:
  - $5^1 \bmod 23 = 5$
  - $5^2 \bmod 23 = 2$
  - $5^3 \bmod 23 = 10$
  - …
  - $5^6 \bmod 23 = 8$ YES!
- Eve now gets shared secret the same way Alice does using Bob's public key:
- $19^6 \bmod 23 = 2$ YES!
- Finding discrete logarithms of 600 digit primes is *very* hard

Man-in-the-middle attack



- Diffie Hellman has no authentication
- Alice cannot be sure she is talking to Bob!
- Frank can get in the middle and impersonate them both
- Only secure against passive attack

What we discussed

- Key distribution challenges
- Public-key cryptography
  - Encryption
  - Signature
  - Public/private key pairs
- Diffie-Hellman key exchange
  - Modular math and discrete logarithms
- Man-in-the-middle attack

What's next

- Module 3 continued: Public Key Cryptography and Digital Signature
- Readings
  - Anderson, Chapter 5 on Cryptography (especially 5.7 Asymmetric Crypto Primitives)
  - Optional Menezes et al, Chapter 1 Overview of Cryptography
  - Optional: Menezes et al, detailed reference information on ciphers in Chapters 7 and 8
- You should be working on Assignment 3 Public Ciphers due next Tuesday
- #breach-of-the-week – participate on slack!
- Office hours Thurs 11:10am-Noon in 192-333 or M/W/F on zoom

Breach of the Week!

RSA public-key crypto

- Named after Rivest, Shamir, and Adleman of MIT in 1977
  - Key exchange
  - Encryption/decryption
  - Digital signature
- Key length: variable bit size (1024, 2048, 4096, and larger)
- Based on difficulty of factoring large numbers
- As much as 200x slower than symmetric key algorithms at equivalent key strength
- Applications
  - Used for short message encryption, digital signature, and secret key exchange

RSA public-key algorithm

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

- p = 17 and q = 11
- n = 17 x 11 = 187
- ϕ(187) = 16 x 10 = 160
- Select *e* relatively prime to 160 and *e* < 160; we choose *e* = 7
- d = 23 because 23 x 7 mod 160 = 1
- PU = {7, 187}
- PR = {23, 187}

- Select plaintext M = 88

- Ciphertext C = 88^7 mod 187 = 11

- Plaintext M = 11^{23} mod 187 = 88

ϕ(n) is Euler totient function

Eve's brute force attack to find private key

- p = 17 and q = 11
- n = 17 x 11 = 187
- $\phi(187) = 16 \times 10 = 160$
- Select *e* relatively prime to 160 and *e* < 160; we choose *e* = 7
- d = 23 because 23 x 7 mod 160 = 1
- PU = {e, n} = {7, 187}
- PR = {d, n} = {23, 187}

- Select plaintext M = 88

- Ciphertext $C = 88^7 \bmod 187 = 11$

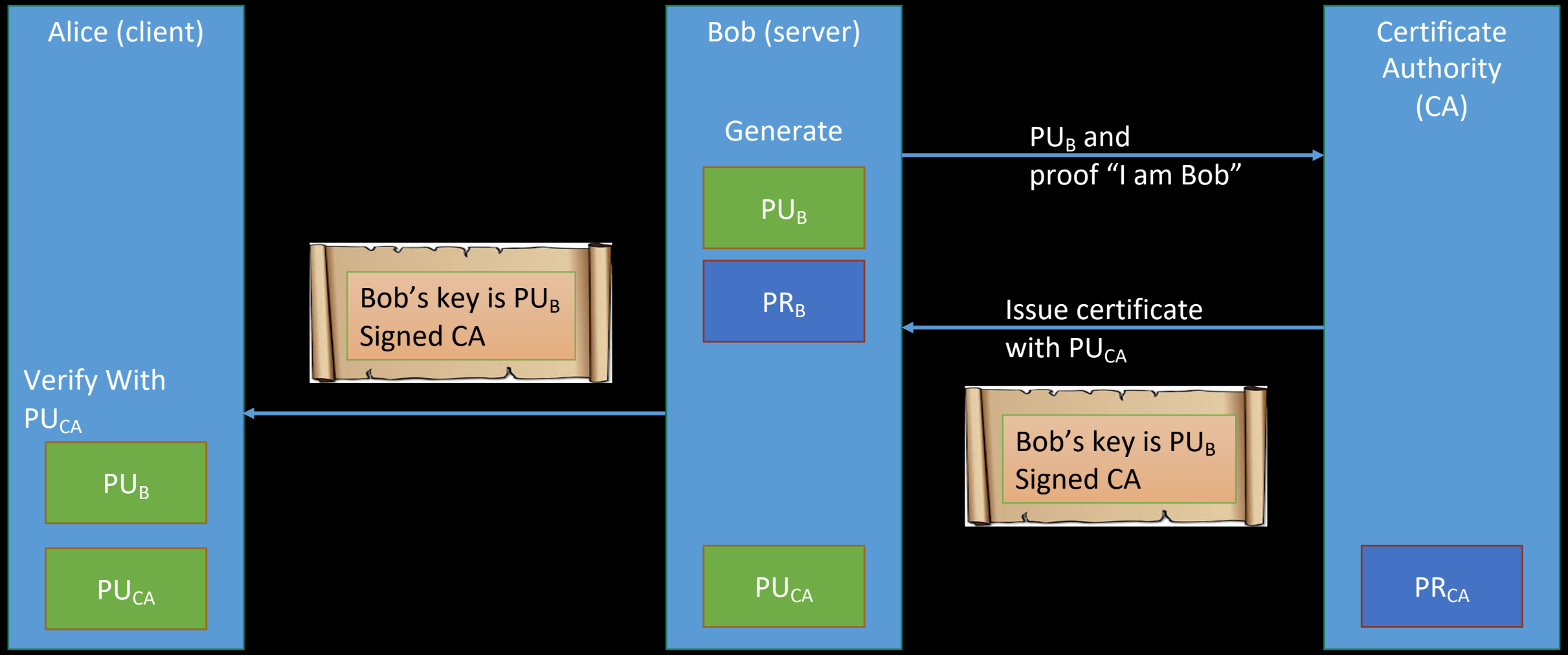
- Plaintext $M = 11^{23} \bmod 187 = 88$

ϕ(n) is Euler totient function

- Eve needs to find Bob's private key:
- Knowing PU = {e, n} = {7, 187}
- Factor n = 187 into its two prime factors
- After lots of work Eve determines 17 x 11 = 187
- $\phi(187) = 16 \times 10 = 160$
- $d \equiv e^{-1} (\text{mod } \phi(n)) \equiv 7^{-1} (\text{mod } 160) \equiv 23$ YES!
- Eve now knows PR = {23, 187}
- Eve can decrypt any messages to Bob using Bob's private key
- But factoring 600 digit product of primes is *very* hard
- Attacks based on running time of the decryption algorithm are also possible!!

Public-key certificates

Bob's certificate is used for a long time (a year) to prove he owns PU_B



#enterprise-group-exercises

- For your enterprise group, what would be the impact to your organization of a Certificate Authority private key breach, and how would you recover?
- Describe the CA breach impact and recovery steps in the #enterprise-group-exercises slack channel

1. Healthcare
2. Government
3. Retail
4. Banking
5. Utility
6. Information Technology
7. University
8. Manufacturing

Elliptic-Curve Cryptography (ECC)

- Uses discrete logarithms on an elliptic curve
  - $y^2 = x^3 + ax + b$
- Property of the curve allows an operation that can be used for cryptography
- Better performance vs RSA
  - Equal security at far smaller bit size
- ECDH – Elliptic-curve Diffie-Hellman
- ECDSA – Elliptic-curve Digital Signature Algorithm

Quantum-resistant cryptography

- Sufficiently powerful quantum computer could solve:
  - Integer factorization (RSA)
  - Discrete logarithm (Diffie-Hellman)
  - Elliptic-curve discrete logarithm (ECC)
- Most symmetric algorithms and hash functions are still secure
- Known quantum computers are not close to breaking algorithms, but unknown how soon threat may appear
- Research underway for public key algorithms that are secure attack by quantum computers
- NIST post-quantum cryptography standardization
  - Evaluation of candidates: lattice, code-based, multivariate types
  - Results hoped to published in 2024 unless sped up by quantum computing breakthrough
  - NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

July 05, 2022

Type	PKE/KEM	Signature
Lattice	• CRYSTALS-Kyber	• CRYSTALS-Dilithium • Falcon
Hash-based		• SPHINCS+

Current NIST guidelines

Date	Security Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A) Digital signatures	Hash (B) HMAC, KMAC
Legacy (1)	80	2TDEA	1024	160	1024	160	SHA-1 (2)	
2019 - 2030	112	(3TDEA) (3) AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

https://www.keylength.com/en/4/

Public-key crypto summary

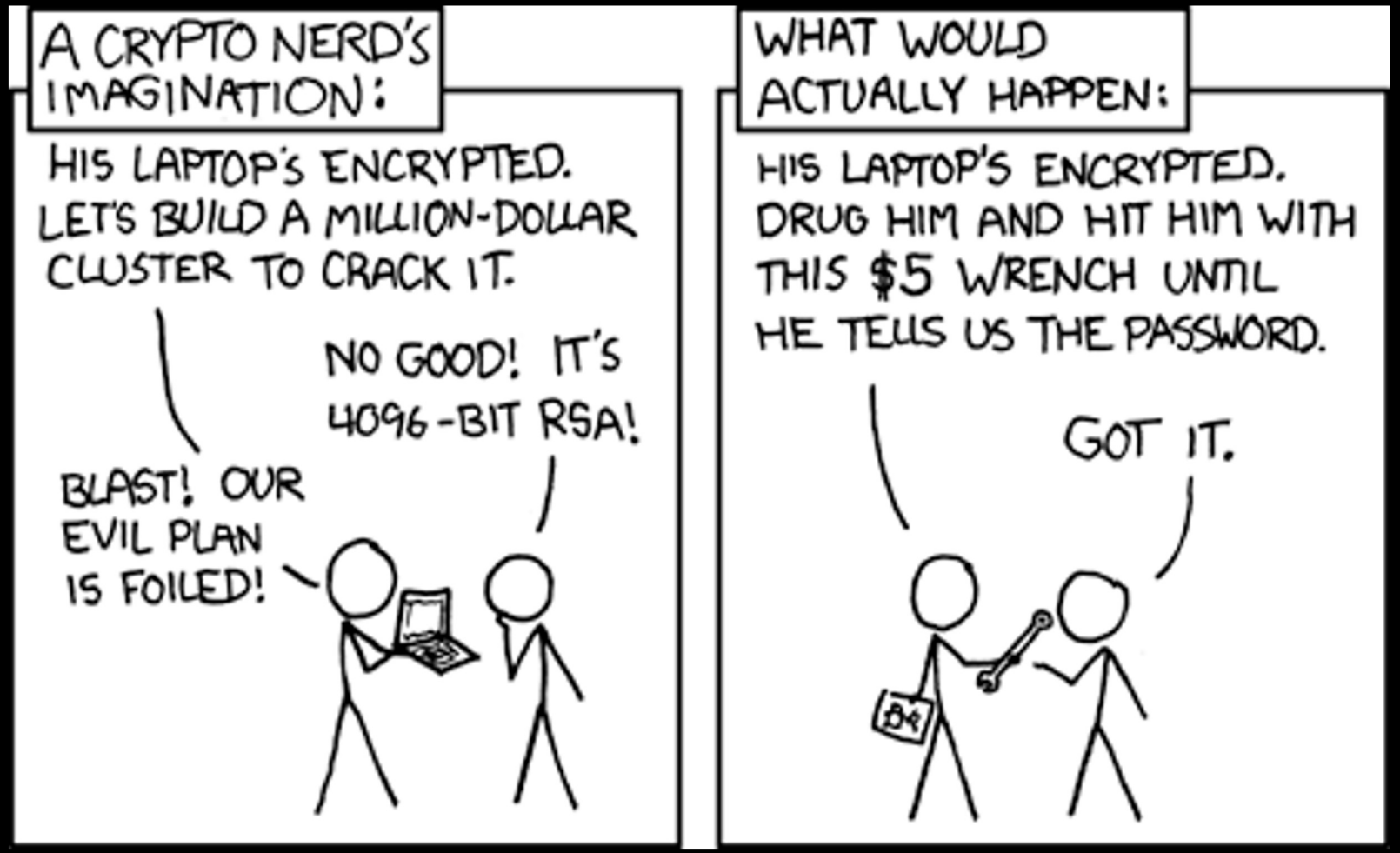
- Advantages
  - Only private key must be kept secret – but authenticity of public keys must be guaranteed!
  - Key administration does not have access to private keys
  - Private/public key pair may last for many years
  - Digital signatures are efficient
  - The number of keys in a large network is much smaller than for symmetric keys
- Disadvantages
  - Encryption is orders of magnitude slower than symmetric
  - Large keys
  - Relies on unproven number-theoretic assumptions

Public-key crypto misconceptions

The following are *not* true:

- Public-key is more secure than symmetric encryption
- Public-key has made symmetric encryption obsolete
- Key distribution is easy with public-key

Reality of cryptography



XKCD 538

Implementing cryptography is not easy

- Implementation challenges
  - Poor secrets (password, key) management
  - Weak Pseudorandom Number Generation
  - Use of Insecure Cryptography
- In the “Top3” of application flaws
  - Data protection regulations have grown increasingly complex

What should you do with crypto?

- Do
  - Understand the tools – not every problem needs a hammer
  - Use tested and trusted implementations
  - Wait for new and exciting improvements to be tested

- Don’t
  - Try to solve all security problems with cryptography: security ≠ crypto
  - Use custom implementations

What we discussed

- RSA public-key algorithm
- PKCS examples
- Public-key certificates
- ECC
- Quantum-resistant crypto
- NIST crypto guidelines
- Public-key advantages/disadvantages
- Reality of implementing cryptography

What's next

- Module 4 User Authentication
- Readings
  - Anderson, Chapter 2 especially 2.4 Passwords, 2.5 System Issues
  - Optional Reading - Securely Storing Passwords
  - Optional reading - n-auth
- Quiz 3, Assignment 3 Public Ciphers due on Tuesday
- #breach-of-the-week – participate on slack!
- Office hours Thurs 11:10am-Noon in 192-333 or M/W/F on zoom