Lecture 21: Key Exchange, Public Key Encryption

Professor Adam Bates
CS 461 / ECE 422
Fall 2019

Goals for Today

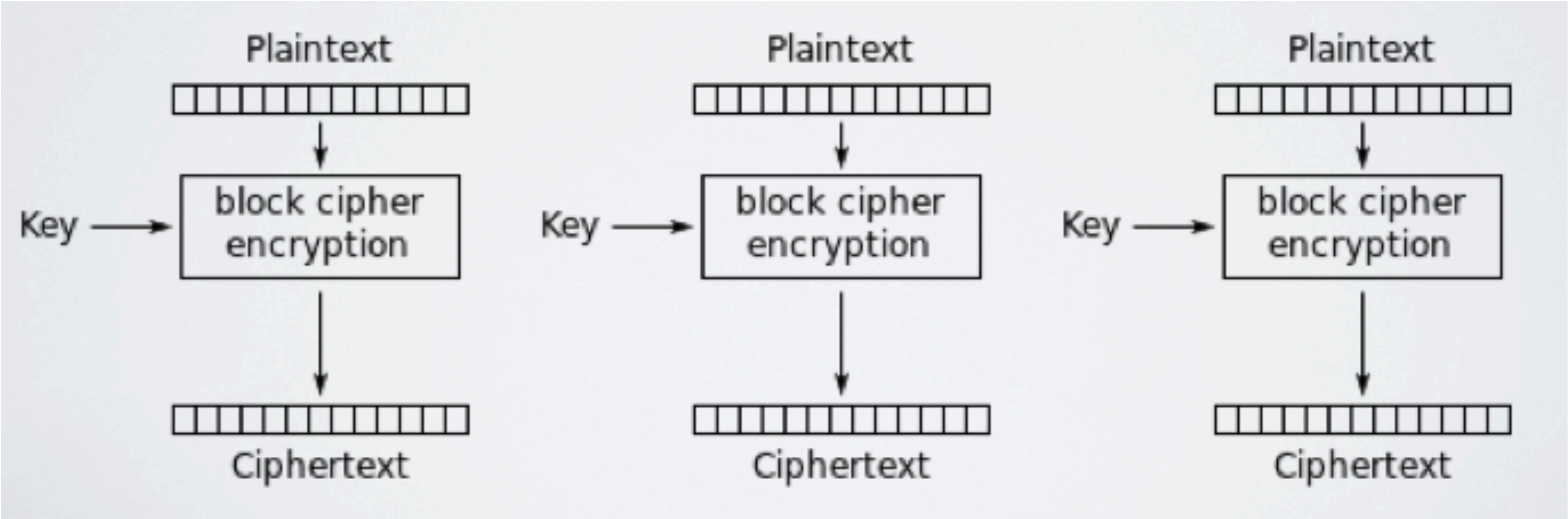
- Learning Objectives:
  - Understand different methods for message confidentiality

- Announcements, etc:
  - MP3 Checkpoint #2: Wednesday Oct 23 at 6pm
  - **Oct 23 Lecture:** *Special Guest Lecture on Human Factors!*

Reminder: Please put away devices at the start of class

Block Ciphers

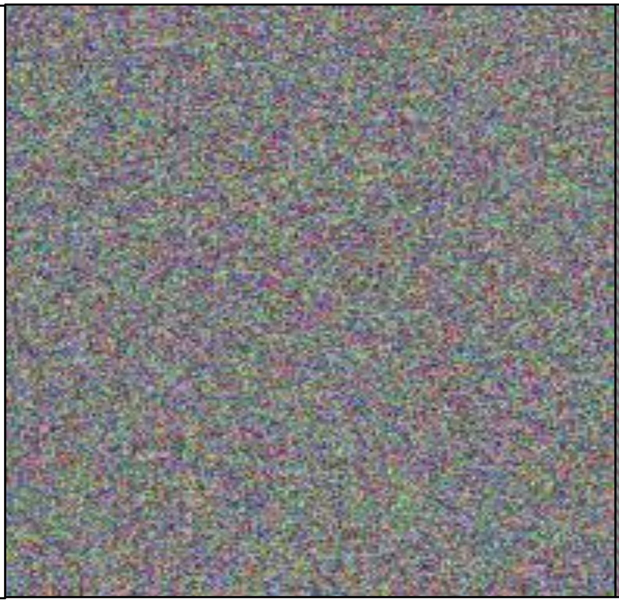
- Several modes of operation for longer messages
- **Electronic Code Book (ECB) Mode:** basically, encrypts each block separately.
- Avoid — why?



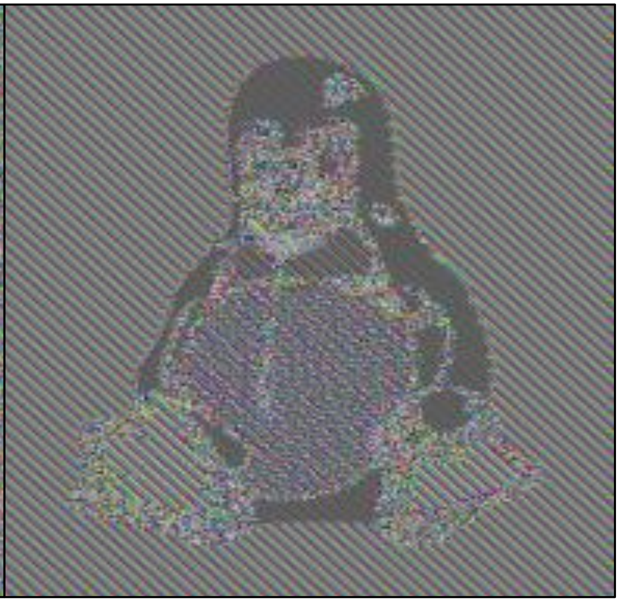
Block Ciphers

- Several modes of operation for longer messages
- **Electronic Code Book (ECB) Mode:** basically, encrypts each block separately.
- Avoid — why?

Plaintext



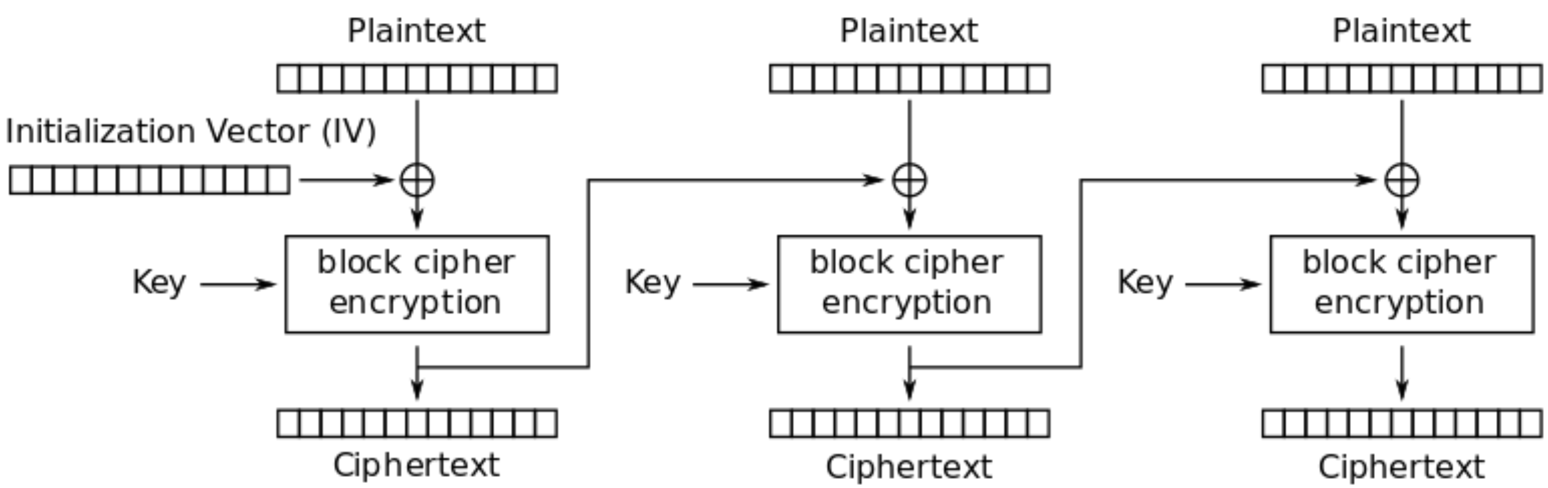
Pseudorandom



ECB mode

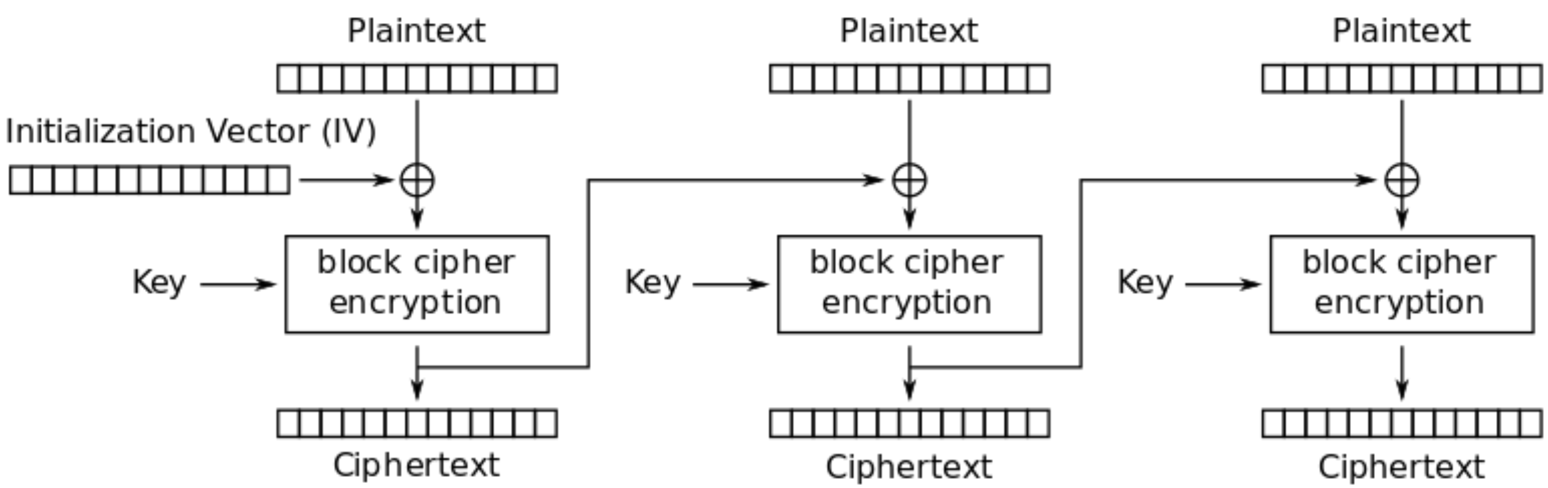
Block Ciphers

- **Cipher Block Chaining (CBC) Mode**: XOR the last cipher block into the next plaintext.
- Use random **Initialization Vector (IV)** for the first block in lieu of a previous cipher block.
- Subtle attack possible if attacker knows IV, controls plain text. [Other Disadvantages?]



Block Ciphers

- **IV Reuse Attack**
  - Early implementations of CBC reused the last cipher text block as the IV for the next message
  - What if attacker gets to see previous encryption before? Is CBC secure against Chosen-Plaintext Attack?

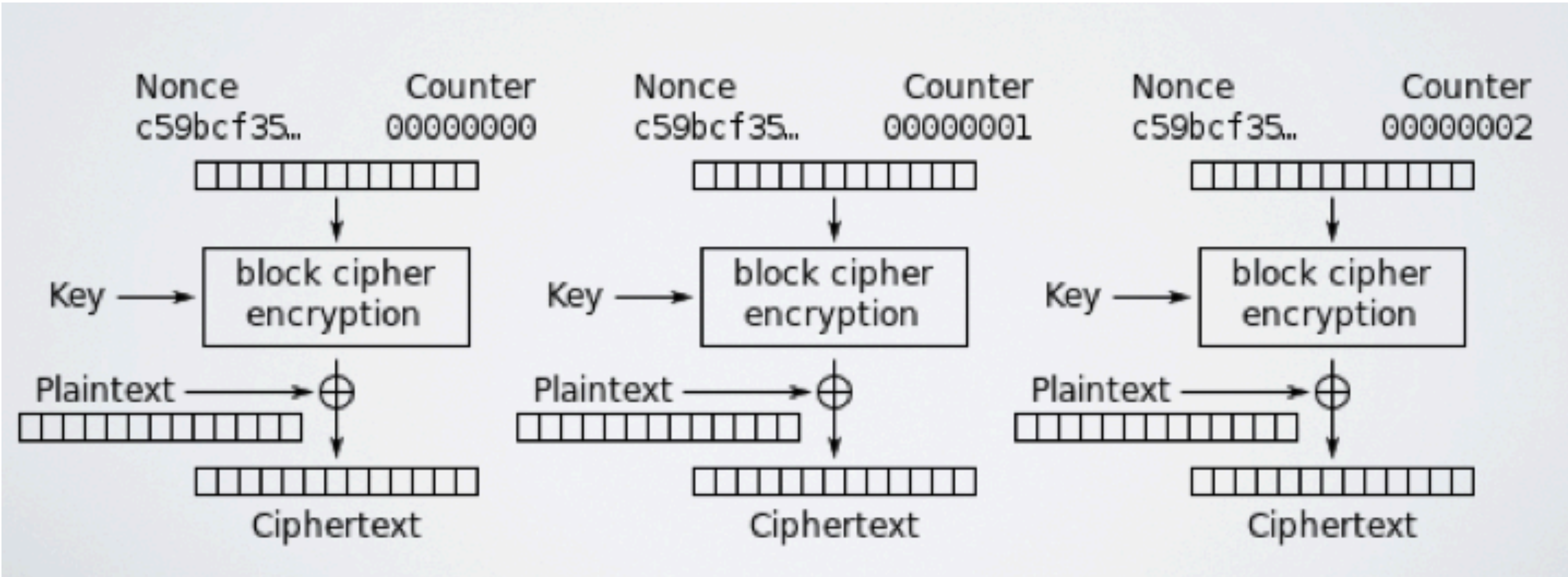


Block Ciphers

- **Padding Oracle Attack on CBC**
  - CBC Decryption: Decrypt all blocks, validate the padding, remove padding, return message.
  - Padding incorrect? <u>Return "Decryption Failed," not "Invalid Padding!"</u>
  - Otherwise, he attacker can use the server as a padding oracle to decrypt (and sometimes encrypt) messages.

Block Ciphers

- **Counter Mode (CTR)**: Generate next key stream block by encrypting successive values of a counter
- Block cipher becomes stream cipher
- Why is nonce (i.e., Message ID) needed?
- Advantages?



From the command line…

Generates a random string

```
$ KEY=$(openssl rand -hex 16)

$ openssl aes-256-cbc -in mymsg.txt -out mymsg.enc
-p -K ${KEY} -iv $(openssl rand -hex 16)
   key=8582D9E1A36DA4DB065394FB1F401DB3
   iv =DBB272FE6486C4D9B09DBE464E080468
```

Prints the key and IV

```
$ openssl aes-256-cbc -d -in mymsg.enc -out mymsg.txt   -K
${KEY} -iv <iv from above>
```

- By default, uses the standard padding described earlier
- Unfortunately, you have to handle prepending/extracting the IV on your own

Definition: a cipher is “Semantically Secure”

Similar game to PRF/PRG/PRP definition:

1. We flip a coin secretly to get a bit **b**, random secret **k**
2. Mallory chooses arbitrary $\mathbf{m_i}$ in **M**, gets to see $\boldsymbol{Enc_k}(\mathbf{m_i})$
3. Mallory chooses two messages $\mathbf{m'_0}$ and $\mathbf{m'_1}$ not in **M**
4. If **b**=0, let **c** be $\boldsymbol{Enc_k}(\mathbf{m'_0})$

   If **b**=1, let **c** be $\boldsymbol{Enc_k}(\mathbf{m'_1})$
5. Mallory can see **c**
6. Mallory guesses **b**, wins if guesses correctly

Also known as: IND-CPA “Chosen plaintext attack”

What is not covered by "Semantic Security?"

- "Malleability" attacks
Given just some ciphertexts, can the attacker create new ciphertexts that Bob decrypts to the wrong value?

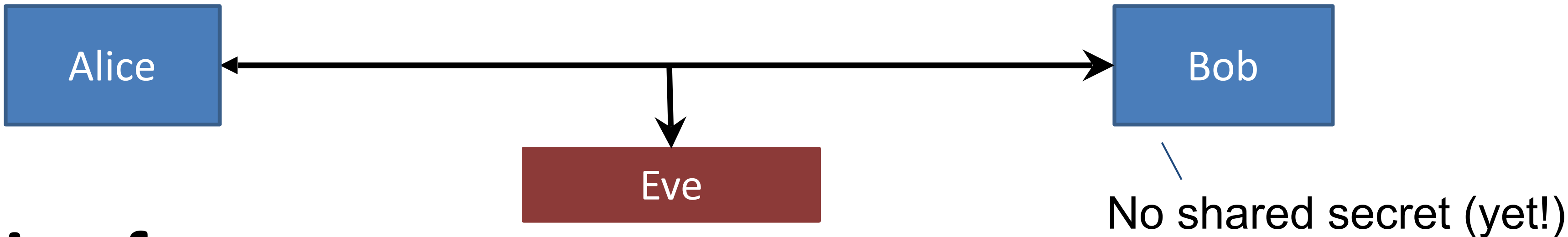
- Encryption does NOT IMPLY integrity!
Often you really want both ("authenticated encryption")

- Chosen Ciphertext attacks
The "semantic security" definition does not allow the adversary to see decryptions of (potentially garbage) ciphertexts chosen by the adversary

- Solution: Encrypt-then-MAC

Key Exchange

Issue: How do we get a shared key?



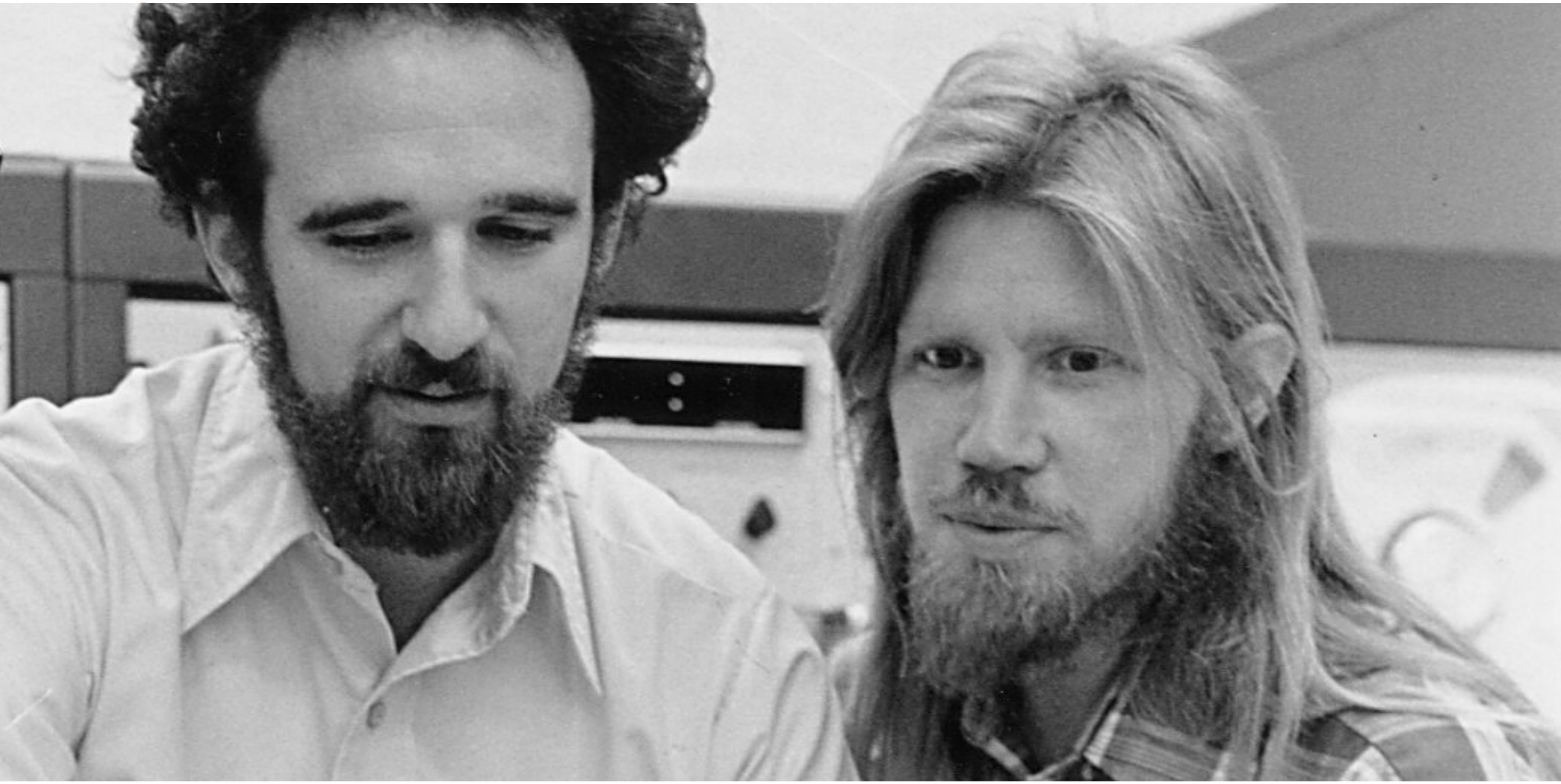
Amazing fact:

Alice and Bob can have a <u>public</u> conversation to derive a shared key!

Diffie-Hellman (D-H) key exchange

1976: Whit Diffie, Marty Hellman, improving partial solution from Ralph Merkle (earlier, in secret, by Malcolm Williamson of British intelligence agency)

Relies on a mathematical hardness assumption called *discrete log problem* (a problem believed to be hard)



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

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Group Theory Basics

Schnorr Groups

A Schnorr group **G** is a subset of numbers, under **multiplication**, modulo a prime **p**.   (a "safe prime")

- We can check if a number **x** is an element of the group
- If **x** and **y** are in the group, then **x y** is in the group too
  (**x y** means **x** times **y** mod **p**)

- **g** is a **generator** of the group if every element of the group can be written as g^x for some exponent x.

g^x

Exponent, $0 <= x < (p - 1)/2$

Generator, an element of the group

What is a Group?

A class of mathematical objects (it generalizes "numbers mod **p**")

Definition: A group (**G**,*) is a set of elements **G**, and a binary operation *

- *(Closed)*: for any $\mathbf{x}, \mathbf{y} \in \mathbf{G}$, we know $\mathbf{x}\ \mathbf{y} \in \mathbf{G}$
- *(Identity)*: we know the identity e in **G**

  for any $\mathbf{x} \in \mathbf{G}$, we have $\mathbf{e}\ \mathbf{x} = \mathbf{x} = \mathbf{x}\ \mathbf{e}$
- *(Inverses)*: for any **x**, we can compute $\mathbf{x}^{-1}\ \mathbf{x} = \mathbf{e}$
- *(Associative)*: For $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{G}$, $\mathbf{x}\ (\mathbf{y}\ \mathbf{z}) = (\mathbf{x}\ \mathbf{y})\ \mathbf{z}$

Schnorr Groups

To generate a Schnorr group:

1. Pick a random, large, (e.g. 2048 bits) "safe prime" $\mathbf{p}$

   $\mathbf{p}$ is a "safe prime" if ($\mathbf{p}$ - 1) / 2 is also prime

2. Pick a random number $\mathbf{g_0}$ in the range 2 to ($\mathbf{p}$ - 1)

3. Let $\mathbf{g} = (\mathbf{g_0})^2 \bmod \mathbf{p}$. If $\mathbf{g} = 1$, loop at step 2

   This is the "generator" of the group.

- A number $\mathbf{x}$ is in the group if $\mathbf{x}^2 \neq 1 \bmod \mathbf{p}$
- The order of each element is (p - 1) / 2.

  $\mathbf{g}^{(p-1)/2} = 1 \bmod \mathbf{p}$
- We can compute inverses $\mathbf{x}^{-1}$ s.t. $\mathbf{x}^{-1}\mathbf{x} = 1 \bmod \mathbf{p}$

Schnorr Groups

Problems assumed "hard" in Schnorr groups:

- Discrete logarithm problem

Given $\mathbf{g}^{\mathbf{x}}$ for some random $\mathbf{x}$, find $\mathbf{x}$

- Diffie Hellman problem (computational)

Given $\mathbf{g}^{\mathbf{a}}$, $\mathbf{g}^{\mathbf{b}}$ for random $\mathbf{a}$,$\mathbf{b}$ compute $\mathbf{g}^{\mathbf{ab}}$

- Diffie Hellman problem (decisional)

Flip a bit *c*, generate random exponents $\mathbf{a}$,$\mathbf{b}$,$\mathbf{r}$

Given ($\mathbf{g}^{\mathbf{a}}$, $\mathbf{g}^{\mathbf{b}}$, $\mathbf{g}^{\mathbf{ab}}$) if c=0, or ($\mathbf{g}^{\mathbf{a}}$, $\mathbf{g}^{\mathbf{b}}$, $\mathbf{g}^{\mathbf{r}}$) if c=1,

Guess *c*

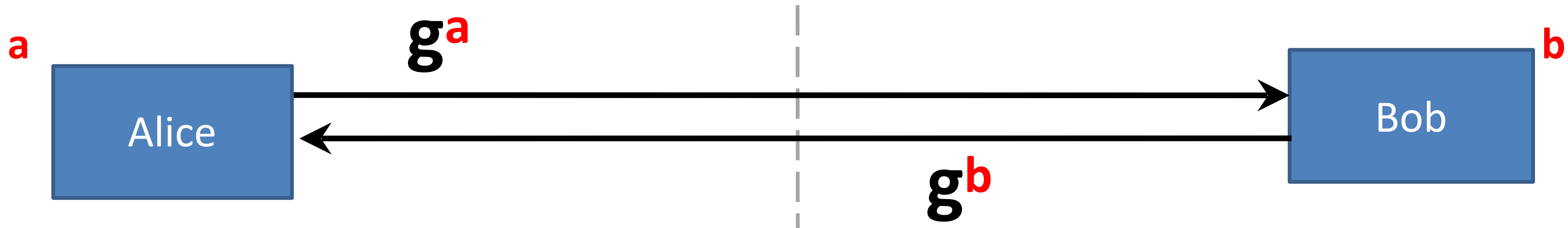
*These problems are thought to be hard in other groups too, e.g. some Elliptic Curves

Diffie-Hellman Protocol

1. Alice and Bob agree on public parameters (maybe in standards doc)

2. **Alice**
   Generates random secret exponent $\mathbf{a}$.

   Bob
   Generates random secret value $\mathbf{b}$.



3. Computes $\mathbf{x}$
   $= (\mathbf{g^b})^{\mathbf{a}}$
   $= \mathbf{g^{ba}}$

   Computes $\mathbf{x'}$
   $= (\mathbf{g^a})^{\mathbf{b}}$
   $= \mathbf{g^{ab}}$

(Notice that $\mathbf{x} == \mathbf{x'}$)

Can use $\mathbf{k}$:= hash($\mathbf{x}$) as a shared key.

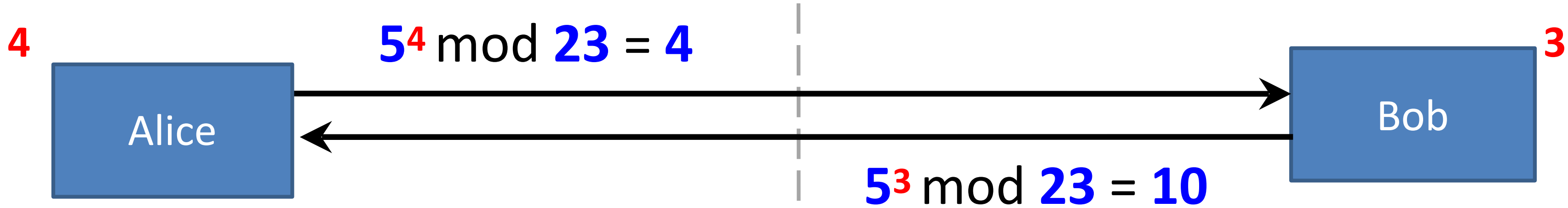
Diffie-Hellman Protocol

1. Alice and Bob agree on public parameters **p=23** and **g=5**

2.

Alice
Generates random secret exponent **4**.

Bob
Generates random secret value **3**.



3.

Alice: Computes **s**

$= 10^4 \bmod 23$

$= 18$

Bob: Computes **s**

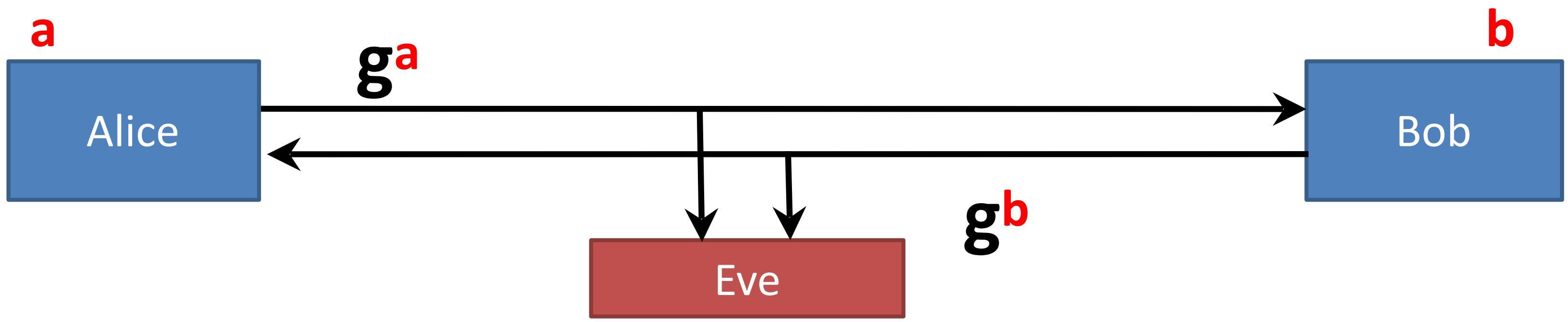
$= 4^3 \bmod 23$

$= 18$

!!!

Diffie-Hellman Protocol

Passive eavesdropping attack



Eve knows: g, g^a, g^b

Eve wants to compute $x = g^{ab}$

Best known approach:

Find a or b, by solving **discrete log**, then compute x

No known efficient algorithm.

[What's D-H's big weakness?]

Man-in-the-Middle (MITM) Attack

Alice does D-H exchange, *really with Mallory*, ends up with g^{au}

Bob does D-H exchange, *really with Mallory*, ends up with g^{bv}

Alice and Bob each think they are talking with the other, but really Mallory is between them and knows both secrets

Bottom line: D-H gives you secure connection, but you don't know who's on the other end!

Defending D-H against MITM

- Cross your fingers and hope there isn't an active adversary.
- Rely on out-of-band communication between users. [Examples?]
- Rely on physical contact to make sure there's no MITM. [Examples?]
- Integrate D-H with user authentication.

  If Alice is using a password to log in to Bob, leverage the password:

    Instead of a fixed **g**, derive **g** from the password – Mallory can't participate w/o knowing password.
- Use digital signatures. [More next week.]

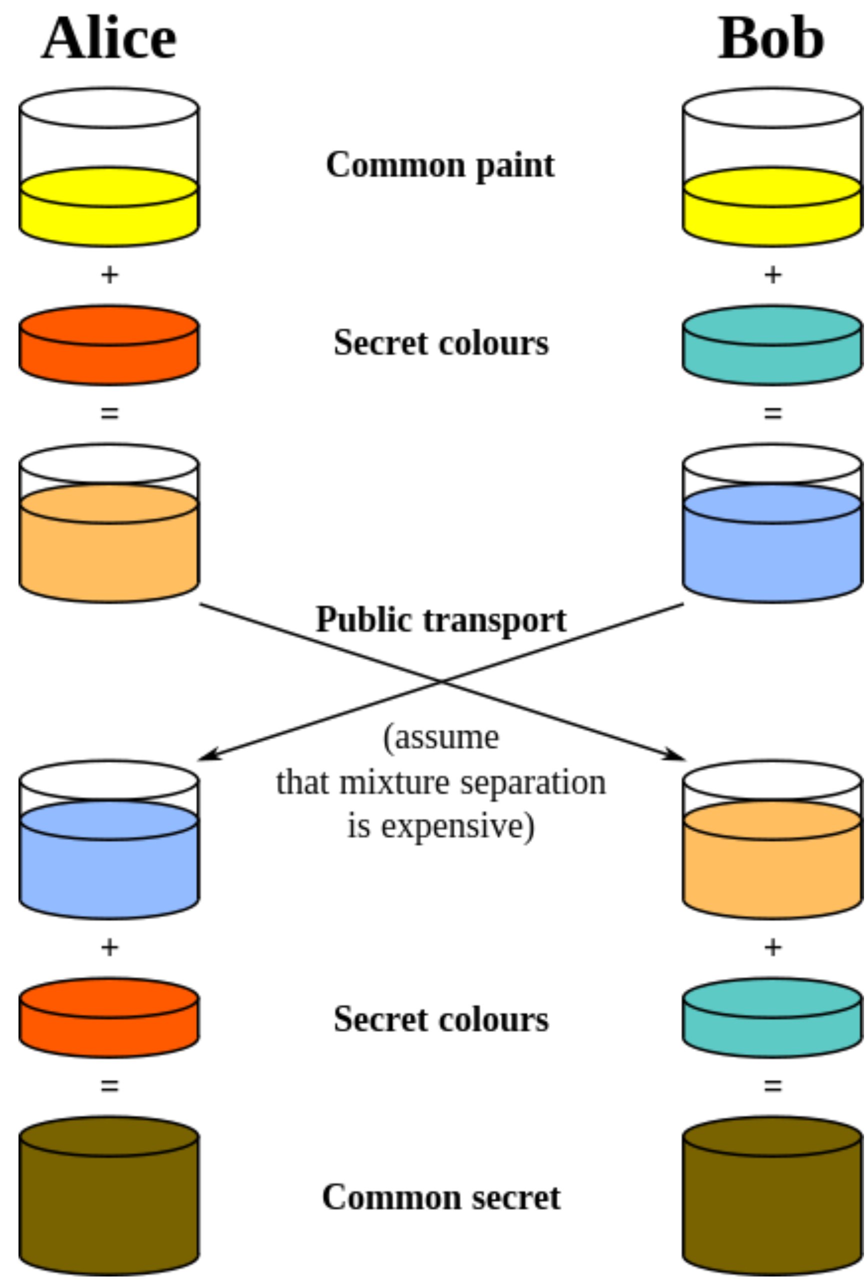
A Visual Analogy

“Mixing paints”

Mixing in a new color is a little bit like exponentiation.

Hard to invert?

Two different ways at arriving at the same final result.



Public Key Encryption

Suppose Bob wants to receive data from lots of people, confidentially…

Schemes we've discussed would require a separate key shared with each person

Example: a journalist who wishes to receive secret tips

Public Key Encryption

- ***Key generation:*** Bob generates a keypair
  public key, $\mathbf{k_{pub}}$ and private key, $\mathbf{k_{priv}}$

- ***Encrypt:*** Anyone can encrypt the message M, resulting in ciphertext C = **Enc**($\mathbf{k_{pub}}$, M)

- ***Decrypt:*** Only Bob has the private key needed to decrypt the ciphertext: M=**Dec**($\mathbf{k_{priv}}$, C)

- ***Security***: Infeasible to guess M or $\mathbf{k_{priv}}$, even knowing $\mathbf{k_{pub}}$ and seeing ciphertexts

Public Key Encryption w/ Ephemeral Key Exchange

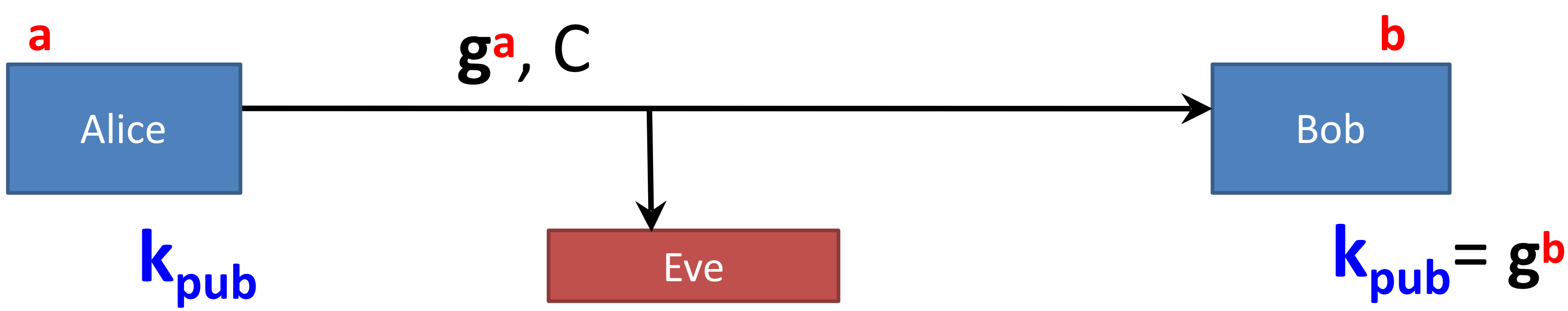
Key generation:

k_{priv}:= b generated randomly, and k_{pub}:= g^b

Encrypt:

Generate random a, set x := hash($k_{pub}{}^{a}$), encrypt C using AES. Send (g^a, C) as ciphertext

Decrypt(g^a, C): compute x = hash($(g^a)^b$), decrypt



Public Key Digital Signatures

Suppose Alice publishes data to lots of people, and they all want to verify integrity…

Can't share an integrity key with *everybody*, or else *anybody* could forge messages

Example: administrator of a source code repository

Public Key Digital Signatures

- Key generation: Bob generates a keypair public key, k_{pub} and private key, k_{priv}

- Bob can sign a message M, resulting in signature S =Sign(k_{priv}, M)

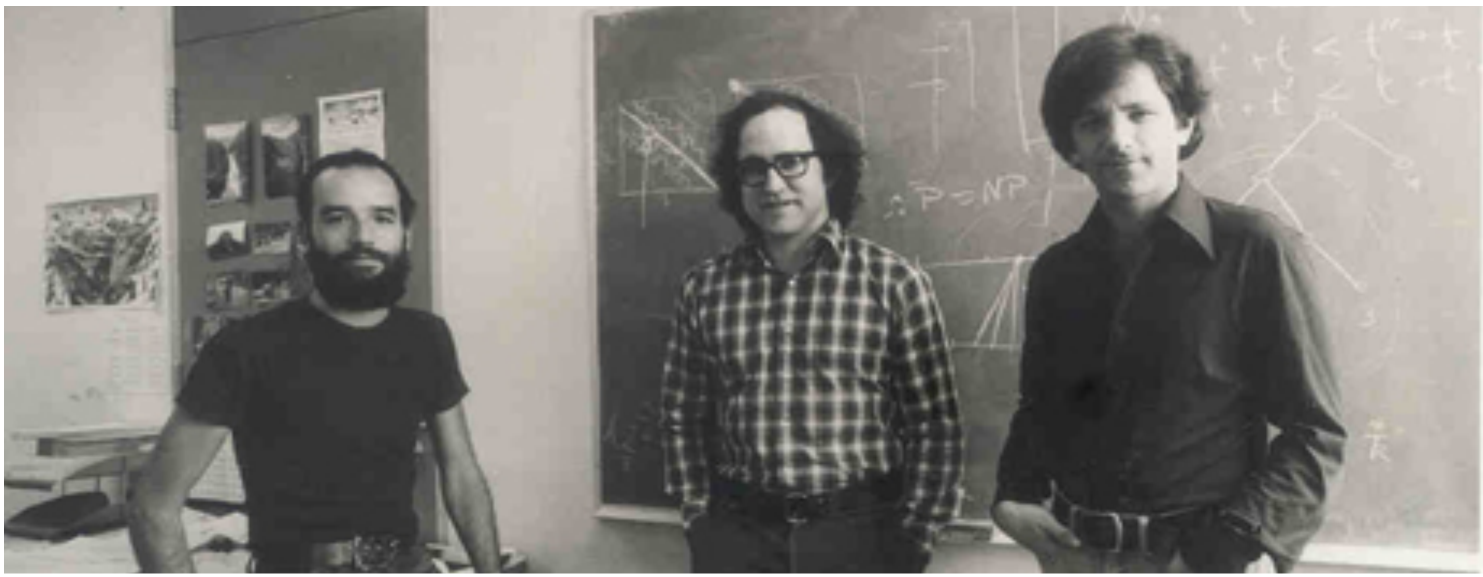
- Anyone who knows k_{pub} can check the signature: Verify(k_{pub}, M, S) =? 1

- "Unforgeable": Computationally infeasible to guess S or k_{priv}, even knowing k_{pub} and seeing signatures on other messages

Public Key Digital Signatures

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*



Best known, most common public-key algorithm: **RSA**

Rivest, Shamir, and Adleman 1978

(earlier by Clifford Cocks of British intelligence, in secret)

How RSA Works

Key generation:

1. Pick large (say, 1024 bits) random primes **p** and **q**
2. Compute **N** := **pq** (RSA uses multiplication mod **N**)
3. Pick **e** to be relatively prime to (**p**-1)(**q**-1)
4. Find **d** so that **ed** mod (**p**-1)(**q**-1) = 1
5. Finally:

Public key is (**e**,**N**)

Private key is (**d**,**N**)

To sign: S = ***Sign***(**x**) = $\mathbf{x}^{\mathbf{d}}$ mod **N**

To verify: ***Verif***(S) = $S^{\mathbf{e}}$ mod **N** Check ***Verif***(S) =? M

How RSA Works

"Completeness" theorem:

For all $0 < \mathbf{x} < \mathbf{N}$, we can show that ***Verif***(***Sign***($\mathbf{x}$)) = $\mathbf{x}$

Proof:

Verif(***Sign***($\mathbf{x}$)) $= (\mathbf{x}^{\mathbf{d}} \bmod \mathbf{pq})^{\mathbf{e}} \bmod \mathbf{pq}$

$= \mathbf{x}^{\mathbf{ed}} \bmod \mathbf{pq}$

$= \mathbf{x}^{\mathbf{a}(\mathbf{p}-1)(\mathbf{q}-1)+1} \bmod \mathbf{pq}$ for some $\mathbf{a}$

(because $\mathbf{ed} \bmod (\mathbf{p}-1)(\mathbf{q}-1) = 1$)

$= (\mathbf{x}^{(\mathbf{p}-1)(\mathbf{q}-1)})^{\mathbf{a}}\mathbf{x} \bmod \mathbf{pq}$

$= (\mathbf{x}^{(\mathbf{p}-1)(\mathbf{q}-1)} \bmod \mathbf{pq})^{\mathbf{a}}\mathbf{x} \bmod \mathbf{pq}$

$= 1^{\mathbf{a}}\mathbf{x} \bmod \mathbf{pq}$

(because of the fact that if $\mathbf{p},\mathbf{q}$ are prime, then for all $0 < \mathbf{x} < \mathbf{N}$,

$\mathbf{x}^{(\mathbf{p}-1)(\mathbf{q}-1)} \bmod \mathbf{pq} = 1$)

$= \mathbf{x}$

Fermat's little theorem

Is RSA Secure?

Best known way to compute **d** from **e**
is factoring **N** into **p** and **q**.

Best known factoring algorithm:
General number field sieve
Takes more than polynomial time
but less than exponential time
to factor **n**-bit number.

(Still takes way too long if **p**,**q**
are large enough and random.)

Fingers crossed…
but can't rule out a breakthrough!

From the command line…

To generate an RSA keypair:

```
$ openssl genrsa -out private.pem 1024
$ openssl rsa -pubout -in private.pem > public.pem
```

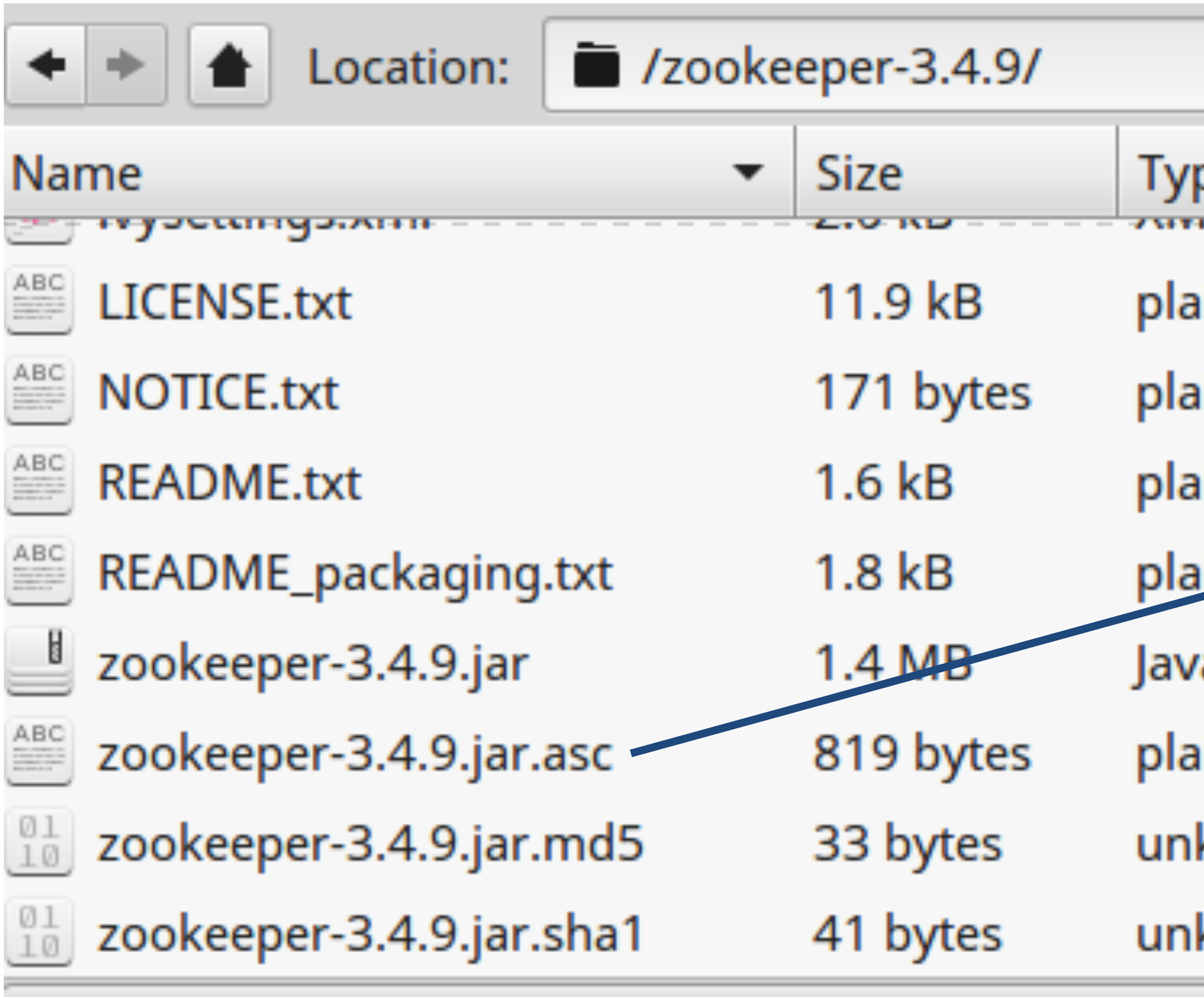
To sign a message with RSA:

```
$ openssl rsautl -sign -inkey private.pem -in a.txt > sig
```

To verify a signed message with RSA:

```
$ openssl rsautl -verify -pubin -inkey public.pem -in sig
```

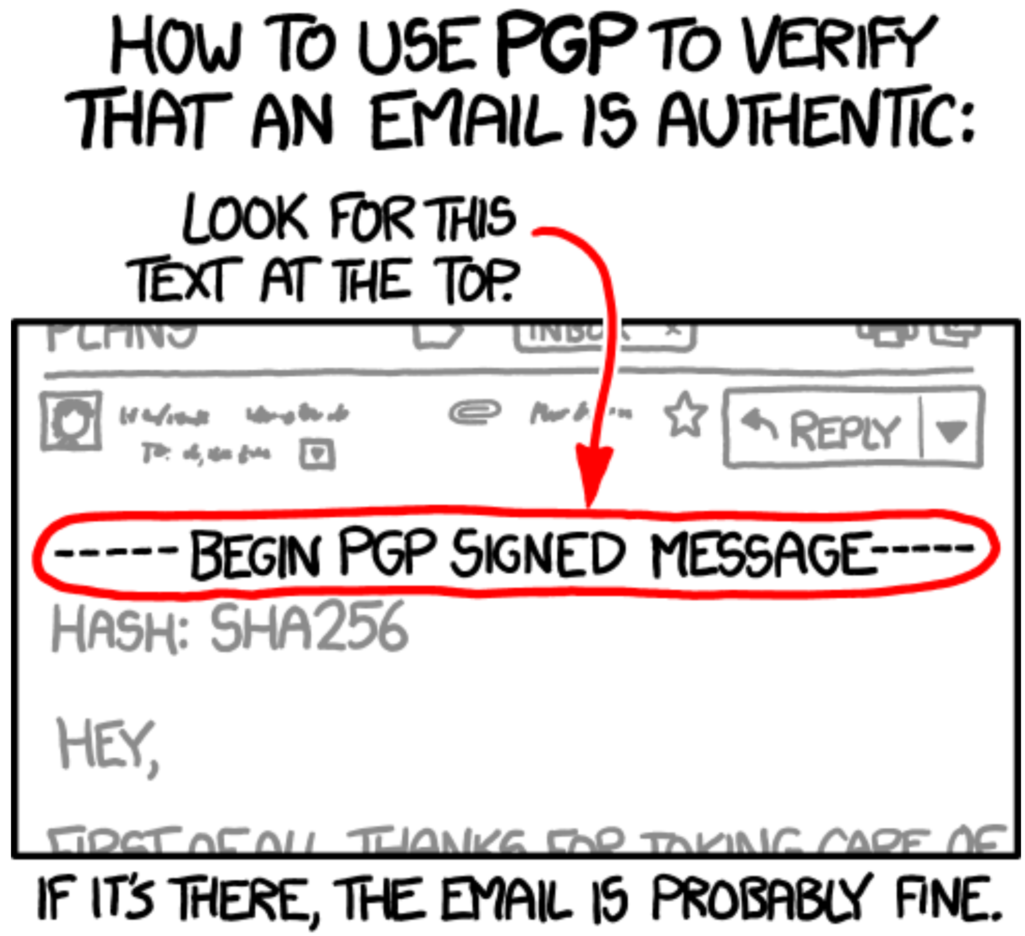
From the command line…



Public key digital signatures on hashes of code releases

Pretty Good Privacy (PGP)

- Another command line tool
- Support for email
- Aside: ***Are these crypto tools usable?***



https://xkcd.com/1181/

Subtle fact: RSA can be used for either confidentiality or integrity

RSA for confidentiality:

Encrypt with public key, Decrypt with private key

Public key is $(\mathbf{e},\mathbf{N})$

Private key is $(\mathbf{d},\mathbf{N})$

To encrypt: $E(\mathbf{x}) = \mathbf{x}^{\mathbf{e}} \bmod \mathbf{N}$

To decrypt: $D(\mathbf{x}) = \mathbf{x}^{\mathbf{d}} \bmod \mathbf{N}$

RSA for integrity:

Encrypt (“sign”) with private key

Decrypt (“verify”) with public key

RSA: Confidentiality or Integrity

Subtle fact: RSA can be used for either confidentiality or integrity

RSA for confidentiality:

Encrypt with public key, Decrypt with private key

Public key is (e, N)

Private key is (d, N)

To encrypt: $E(x) = x^e \bmod N$

To decrypt: $D(x) = x^d \bmod N$

RSA for integrity:

Encrypt ("sign") with private key

Decrypt ("verify") with public key

RSA Performance

Factor of 1000 or more slower than AES.

Dominated by exponentiation – cost goes up (roughly) as cube of key size.

Message must be shorter than **N**.

Use in practice:

Hybrid Encryption (similar to key exchange):

Use RSA to encrypt a random key **k < N**, then use AES

Signing:

Compute **v** := hash(**m**), use RSA to sign the hash

Should **<u>always</u>** use crypto libraries to get details right

What can go wrong with RSA?

Twenty Years of Attacks on the RSA Cryptosystem

Dan Boneh
dabo@cs.stanford.edu

Hundreds of things!!

Many have a common theme: tweaking the protocol for efficiency (e.g., small exponents) leads to a compromise.

What can go wrong with RSA?

One example of a failure: Common P's and Q's

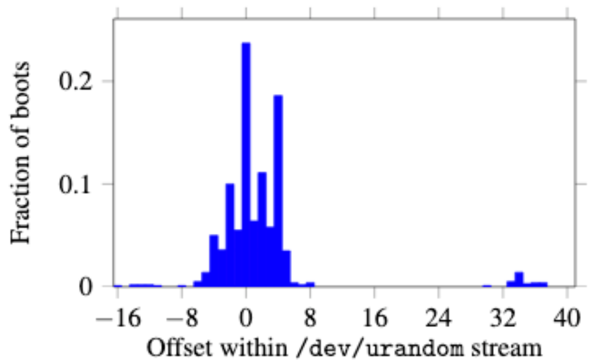
Individually, $N = pq$ is very hard to factor.

Turns out, due to poor entropy, many pairs of RSA keys are generated with same p

$$N_1 = p\,q_1$$

$$N_2 = p\,q_2$$

Given two products with a common factor, easy to compute $GCD(N_1, N_2)$ with Euclid's algorithm.



[Heninger et al., USENIX Security '12]

Cryptography, A Recap

- Don’t roll your own crypto
- Don’t roll your own crypto
- Don’t roll your own crypto
- Don’t roll your own crypto
- Don’t roll your own crypto
- Don’t roll your own crypto
- Don’t roll your own crypto
- Don’t roll your own crypto

Key Management

The hard part of crypto: **Key-management**

Principles:

0. Always remember, key management is the hard part!

1. Each key should have only one purpose
   (in general, no guarantees when keys reused elsewhere)

1. Vulnerability of a key increases:
   a. The more you use it.
   b. The more places you store it.
   c. The longer you have it.

2. Keep your keys far from the attacker.

3. Protect yourself against compromise of old keys.
   Goal: **forward secrecy** — learning old key shouldn't help adversary learn new key.
   [How can we get this?]

Safely Building Secure Channels

What if you want confidentiality and integrity at the same time?

Encrypt, then MAC
not the other way around

Use separate keys for confidentiality and integrity.

- Need two shared keys,
  - but only have one?
  - That's what PRGs are for!
- If there's a reverse (Bob to Alice) channel, use separate keys for that too

How big should keys be?

Want probability of guessing to be infinitesimal… but watch out for Moore's law – safe size gets 1 bit larger every 18 months

128 bits usually safe for ciphers/PRGs

Need larger values for MACs/PRFs due to **birthday attack**

- Often trouble if adversary can find <u>any two messages</u> with same MAC
- Attack: Generate random values, look for coincidence.
- Requires $O(2^{|k|/2})$ time, $O(2^{|k|/2})$ space.
- For 128-bit output, takes 2^{64} steps: doable!

Upshot: Want output of MACs/PRFs to be twice as big as cipher keys e.g. use HMAC-SHA256 alongside AES-128

Key Type *Move the cursor over a type for description*	Cryptoperiod	
	Originator Usage Period (OUP)	Recipient Usage Period
Private Signature Key	1-3 years	-
Public Signature Key	Several years (depends on key size)	
Symmetric Authentication Key	<= 2 years	<= OUP + 3 years
Private Authentication Key	1-2 years	
Public Authentication Key	1-2 years	
Symmetric Data Encryption Key	<= 2 years	<= OUP + 3 years
Symmetric Key Wrapping Key	<= 2 years	<= OUP + 3 years
Symmetric RBG keys	Determined by design	-
Symmetric Master Key	About 1 year	-
Private Key Transport Key	<= 2 years (1)	
Public Key Transport Key	1-2 years	
Symmetric Key Agreement Key	1-2 years (2)	
Private Static Key Agreement Key	1-2 years (3)	
Public Static Key Agreement Key	1-2 years	
Private Ephemeral Key Agreement Key	One key agreement transaction	
Public Ephemeral Key Agreement Key	One key agreement transaction	
Symmetric Authorization Key	<= 2 years	
Private Authorization Key	<= 2 years	
Public Authorization Key	<= 2 years	

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

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

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

Attacks against Crypto

1. Brute force: trying all possible private keys
2. Mathematical attacks: factoring
3. Timing attacks: using the running time of decryption
4. Hardware-based fault attack: induce faults in hardware to generate digital signatures
5. Chosen ciphertext attack
6. Architectural Changes

Btw, Post-Quantum is a thing

Post Quantum:

When will a quantum computer be built?

15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)

What will be impacted?

Public key crypto:

~~RSA~~

~~Elliptic Curve Cryptography (ECDSA)~~

~~Finite Field Cryptography (DSA)~~

~~Diffie-Hellman key exchange~~

Symmetric key crypto:
AES, Triple DES

Need Larger Keys

Hash functions:
~~SHA-1~~, SHA-2 and SHA-3

Use longer output

What's next?

So Far:

Message Integrity

Confidentiality

Key Exchange

Public Key Crypto

Next Week:

HTTPS and TLS: Secure channels for the web

Bitcoin and Cryptocurrencies