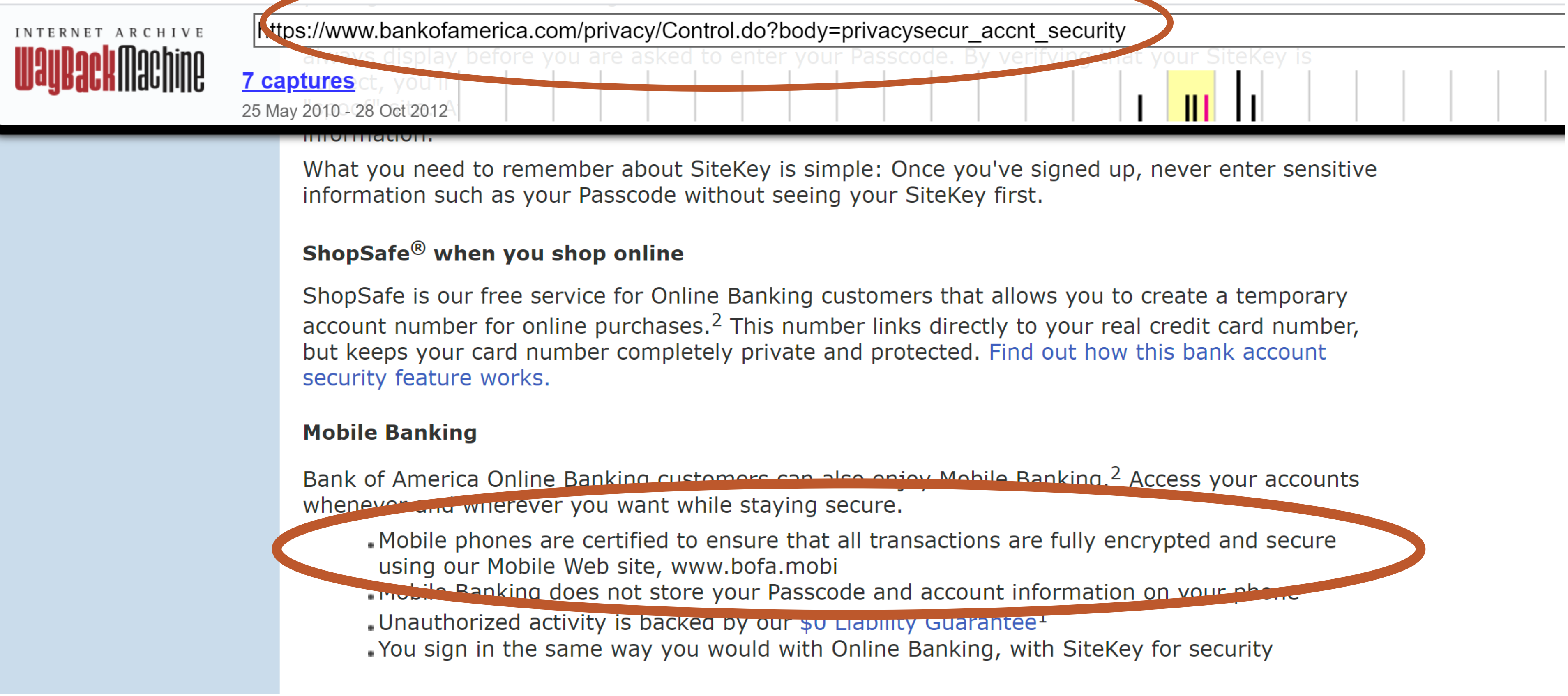
Cryptography in Network Security

UT LAW 379

SPRING 2021

LECTURE NOTES

What is “Cryptography”?



https://www.bankofamerica.com/privacy/Control.do?body=privacysecur_accnt_security

7 captures

25 May 2010 - 28 Oct 2012

always display before you are asked to enter your Passcode. By verifying that your SiteKey is

information.

What you need to remember about SiteKey is simple: Once you've signed up, never enter sensitive information such as your Passcode without seeing your SiteKey first.

ShopSafe® when you shop online

ShopSafe is our free service for Online Banking customers that allows you to create a temporary account number for online purchases.[2] This number links directly to your real credit card number, but keeps your card number completely private and protected. Find out how this bank account security feature works.

Mobile Banking

Bank of America Online Banking customers can also enjoy Mobile Banking.[2] Access your accounts whenever and wherever you want while staying secure.

- Mobile phones are certified to ensure that all transactions are fully encrypted and secure using our Mobile Web site, www.bofa.mobi
- Mobile Banking does not store your Passcode and account information on your phone
- Unauthorized activity is backed by our $0 Liability Guarantee[1]
- You sign in the same way you would with Online Banking, with SiteKey for security

Cryptography ≠ Confidentiality

“Secret” codes usually gets the most attention from non-experts

Websites used to emphasize “security” by talking encryption

In crypto terms, encryption typically provides “confidentiality”

Confidentiality is not the only property, nor even the “most important”

Cryptography Definition

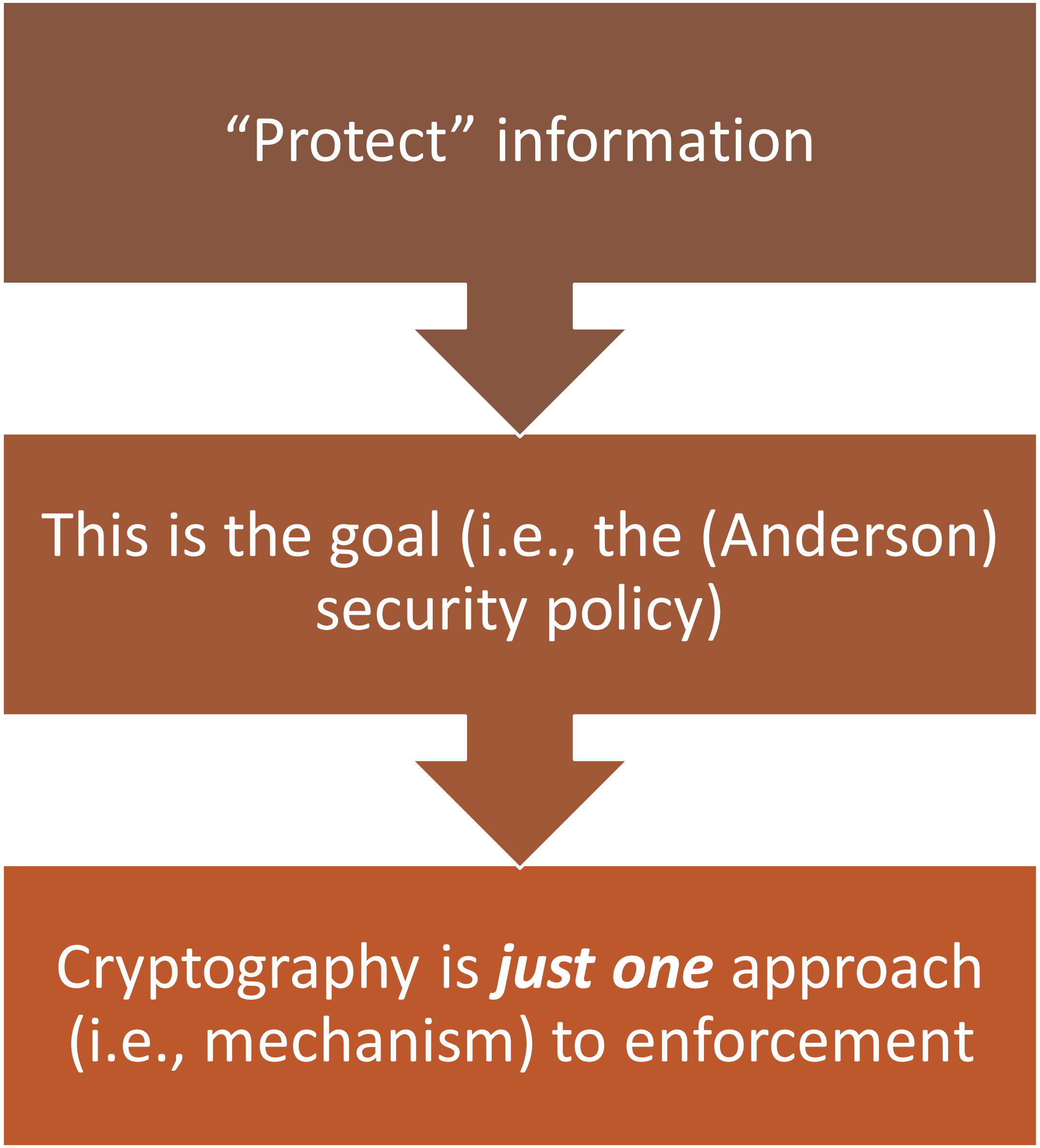
Assume definition of “information” is axiomatic

Study of **mathematical techniques** related to information security such as

- confidentiality,
- data integrity,
- entity authentication, and
- data origin authentication

(See, HAC Definition 1.1)

Information Security

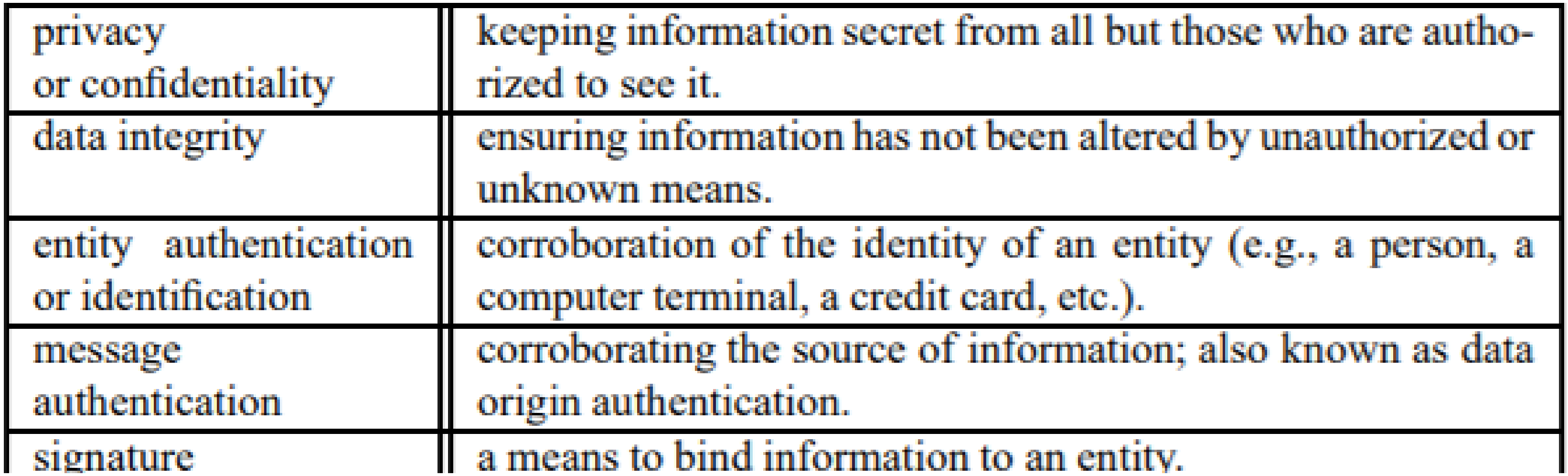


“Protect” information

This is the goal (i.e., the (Anderson) security policy)

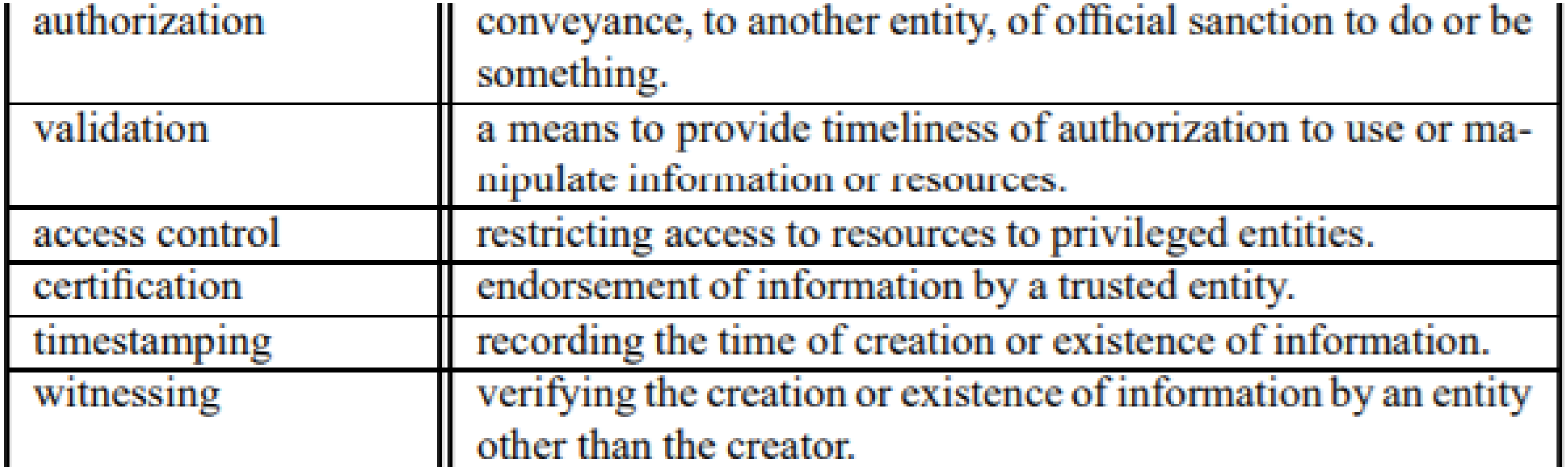
Cryptography is ***just one*** approach (i.e., mechanism) to enforcement

Information Security Objectives



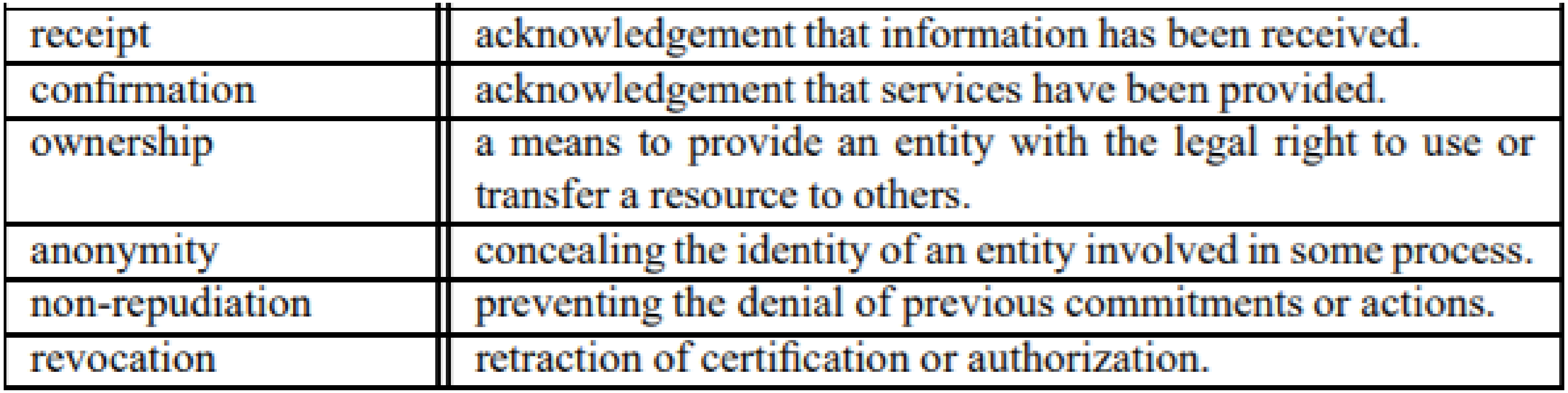
privacy or confidentiality	keeping information secret from all but those who are authorized to see it.
data integrity	ensuring information has not been altered by unauthorized or unknown means.
entity authentication or identification	corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
message authentication	corroborating the source of information; also known as data origin authentication.
signature	a means to bind information to an entity.

Information Security Objectives



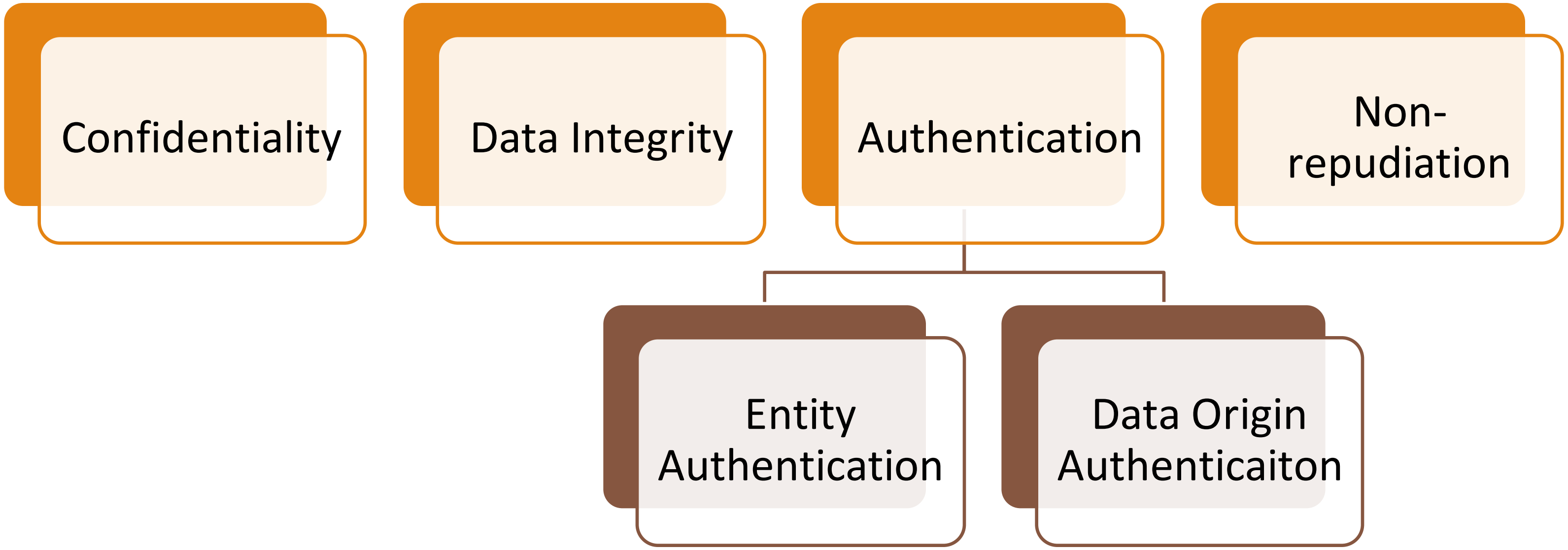
authorization	conveyance, to another entity, of official sanction to do or be something.
validation	a means to provide timeliness of authorization to use or manipulate information or resources.
access control	restricting access to resources to privileged entities.
certification	endorsement of information by a trusted entity.
timestamping	recording the time of creation or existence of information.
witnessing	verifying the creation or existence of information by an entity other than the creator.

Information Security Objectives



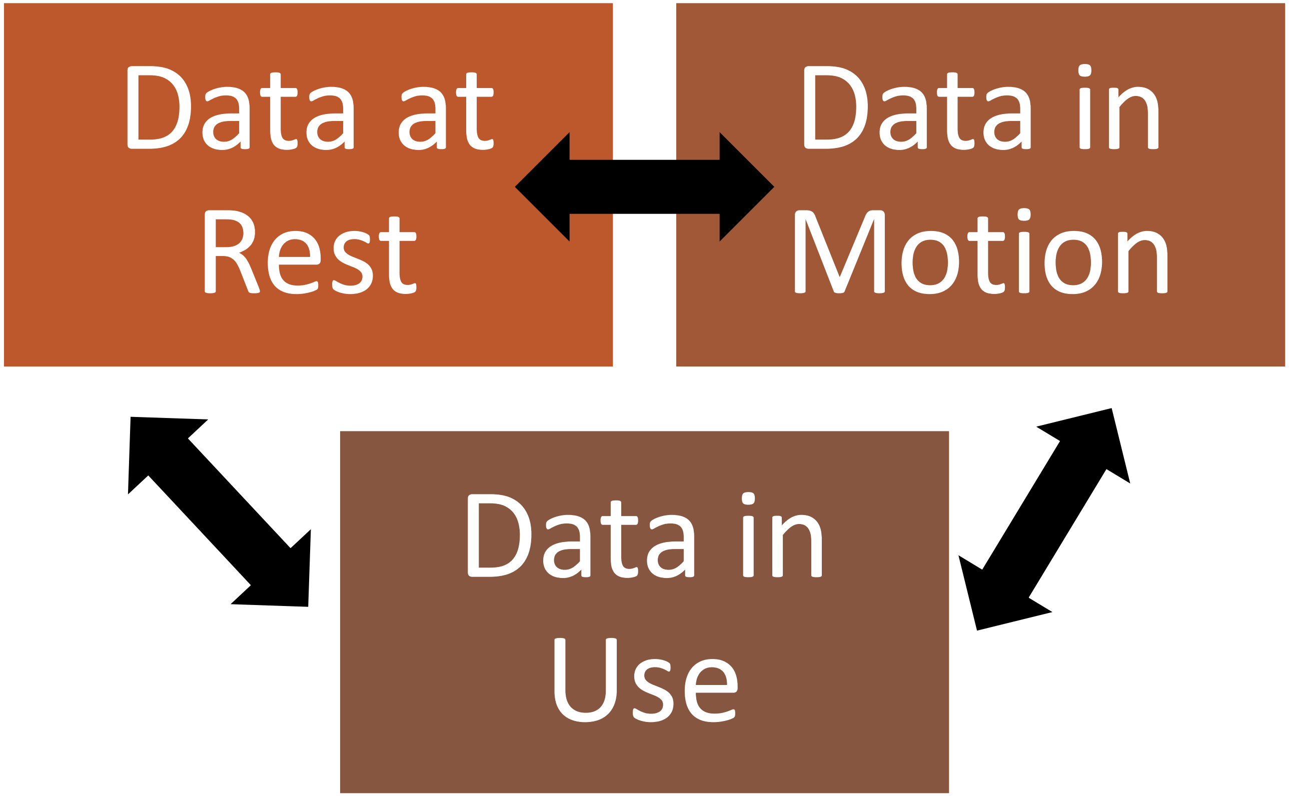
receipt	acknowledgement that information has been received.
confirmation	acknowledgement that services have been provided.
ownership	a means to provide an entity with the legal right to use or transfer a resource to others.
anonymity	concealing the identity of an entity involved in some process.
non-repudiation	preventing the denial of previous commitments or actions.
revocation	retraction of certification or authorization.

Crypto’s Primary Objectives



Other objectives built on top of these four properties

States* of Data



*Analogous to States of Matter (solid, liquid, gas)

Crypto in Network Security

Protecting Data In Motion gets most of the attention

- Common objective: Over-the-network entity authentication
- Common objective: Secure Authenticated Channel

Protecting Data-at-Rest and Data-in-Use from network-based adversaries

- Common objective: Maintain data confidentiality (prevent exfiltration)
- Common objective: Maintain data integrity (prevent tampering)

(* Not a comprehensive list!)

Cryptographic “Primitives”

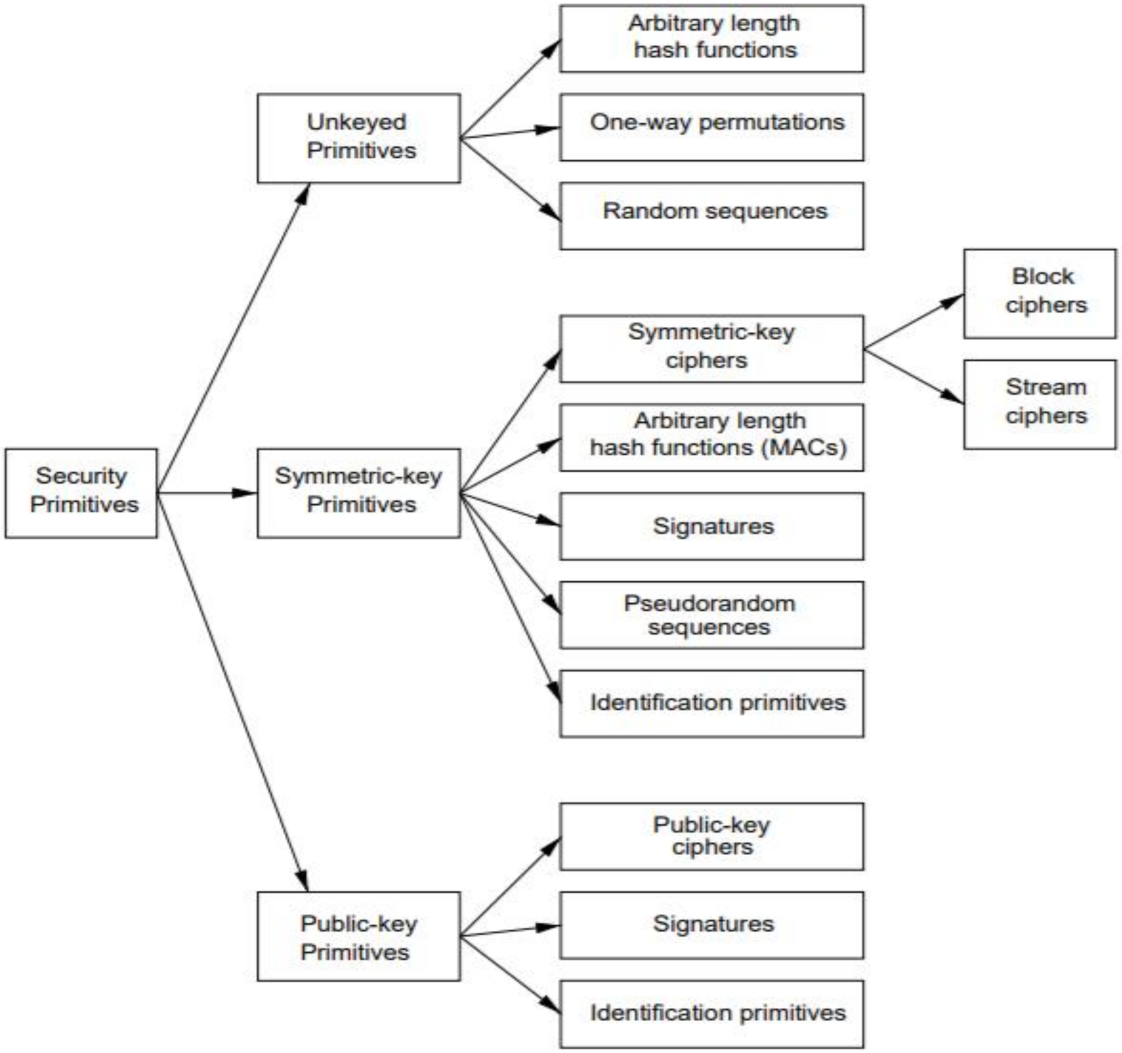
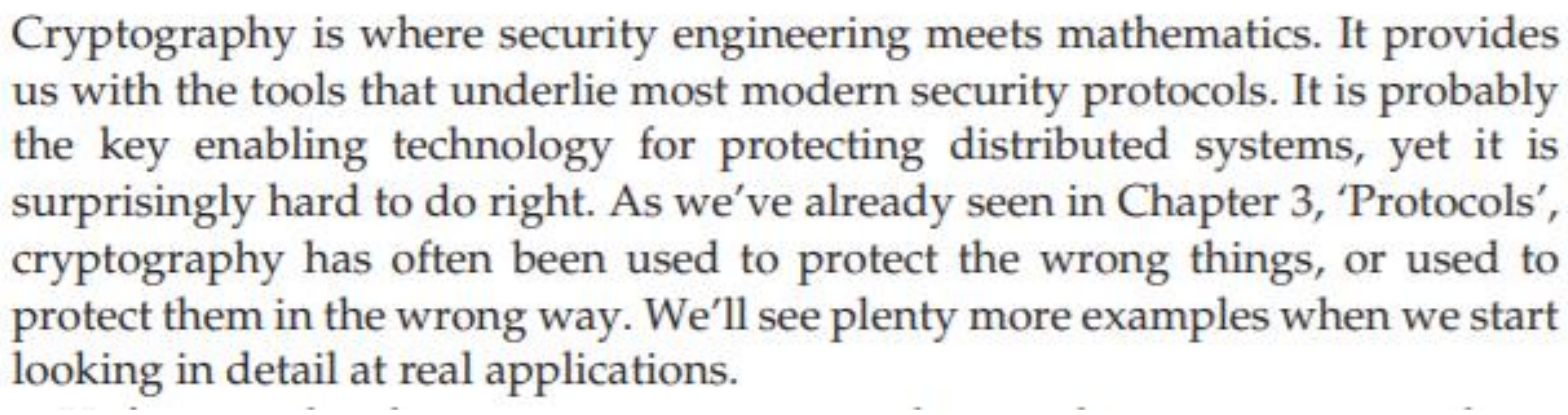


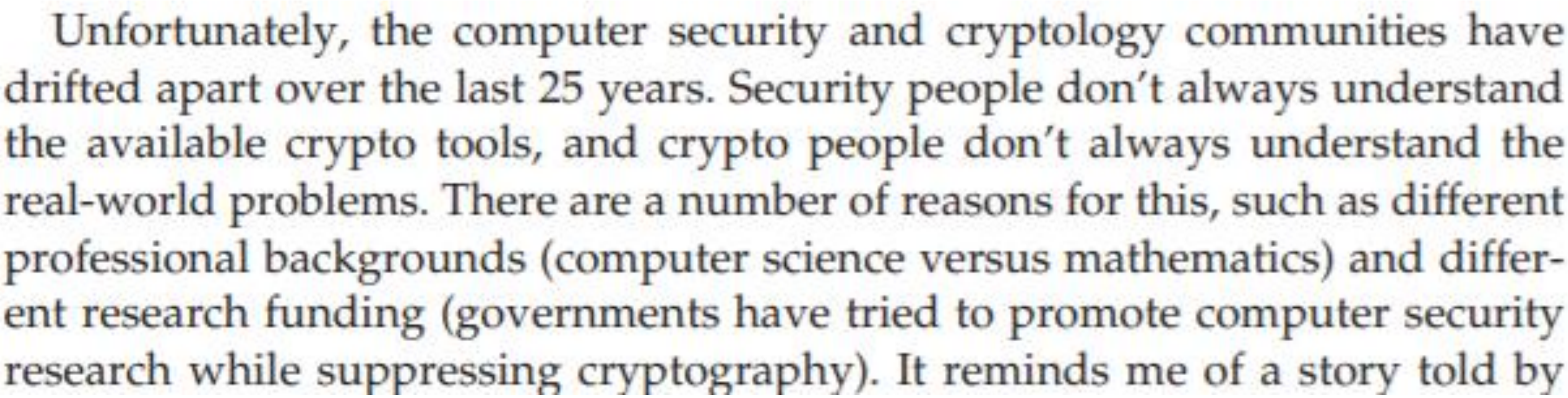
Figure 1.1: *A taxonomy of cryptographic primitives.*

Anderson’s Intro



Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right. As we’ve already seen in Chapter 3, ‘Protocols’, cryptography has often been used to protect the wrong things, or used to protect them in the wrong way. We’ll see plenty more examples when we start looking in detail at real applications.

Security vs Cryptography



Unfortunately, the computer security and cryptology communities have drifted apart over the last 25 years. Security people don't always understand the available crypto tools, and crypto people don't always understand the real-world problems. There are a number of reasons for this, such as different professional backgrounds (computer science versus mathematics) and different research funding (governments have tried to promote computer security research while suppressing cryptography). It reminds me of a story told by

YANAC

YOU ARE NOT A CRYPTOGRAPHER

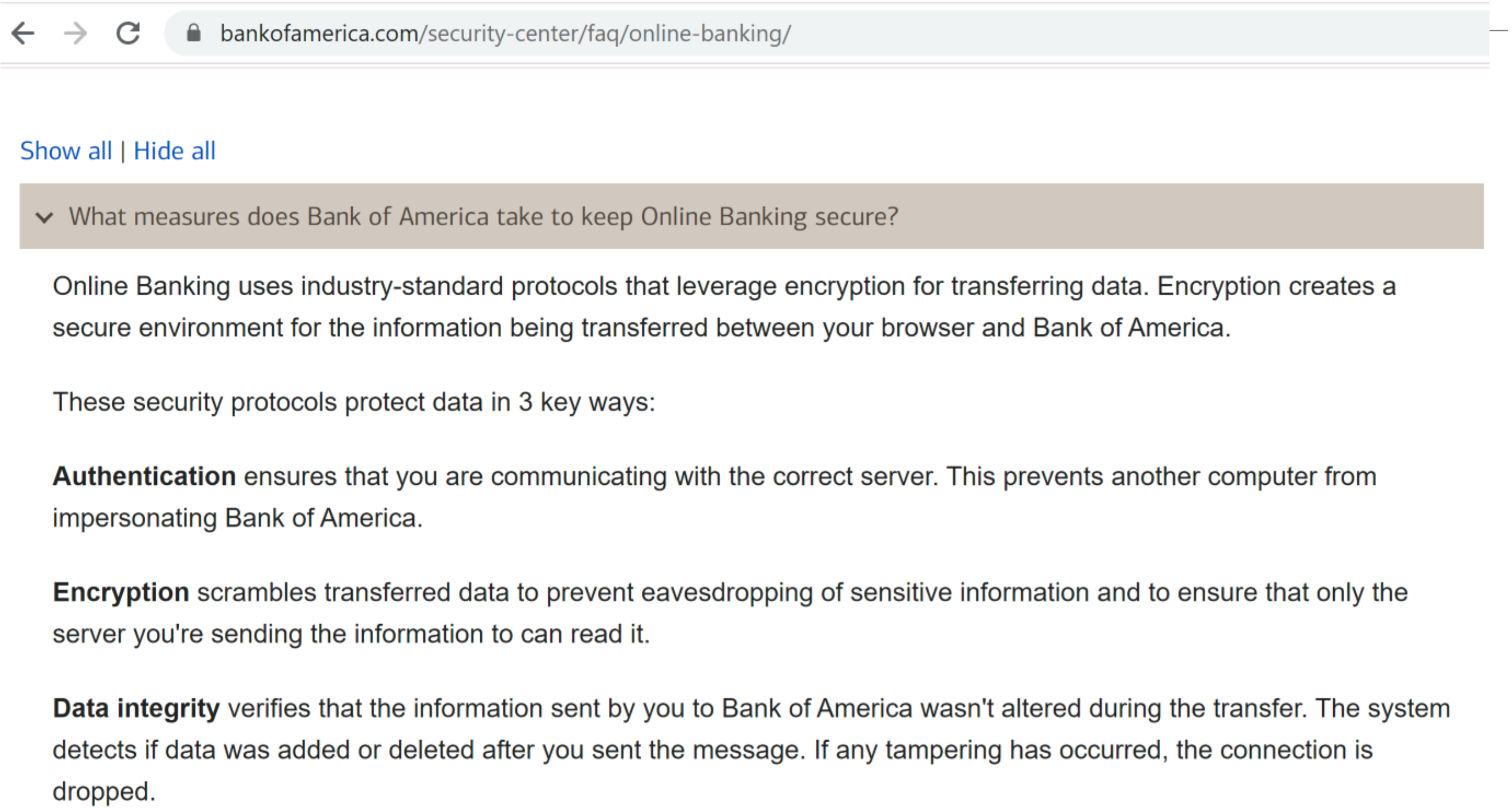
You will acquire ***some*** knowledge in this class

That ***could make you more dangerous, not less!***

Do NOT roll your own cryptography

Know when to tell your boss to hire a cryptography expert

Improvement!



bankofamerica.com/security-center/faq/online-banking/

Show all | Hide all

What measures does Bank of America take to keep Online Banking secure?

Online Banking uses industry-standard protocols that leverage encryption for transferring data. Encryption creates a secure environment for the information being transferred between your browser and Bank of America.

These security protocols protect data in 3 key ways:

Authentication ensures that you are communicating with the correct server. This prevents another computer from impersonating Bank of America.

Encryption scrambles transferred data to prevent eavesdropping of sensitive information and to ensure that only the server you're sending the information to can read it.

Data integrity verifies that the information sent by you to Bank of America wasn't altered during the transfer. The system detects if data was added or deleted after you sent the message. If any tampering has occurred, the connection is dropped.

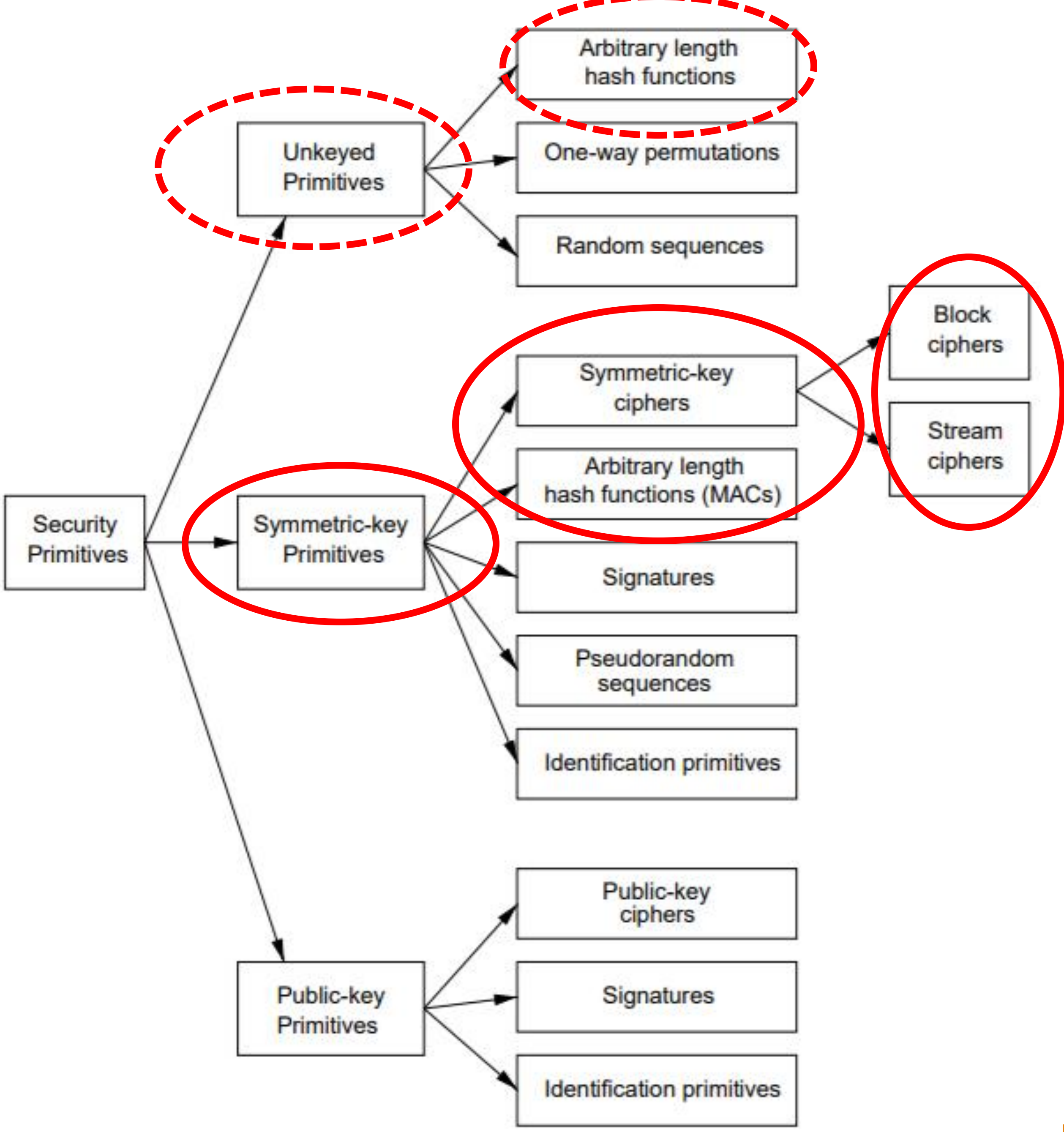


Figure 1.1: *A taxonomy of cryptographic primitives.*

Symmetric Cryptography

All parties in the protocol share a unique key

If |parties| is 1, “secret key”

If |parties| > 1, “shared key”

For today’s examples, assume pre-shared key

Symmetric-Cipher Types

Block Cipher

- Data split in fixed-size blocks
- 1:1 map from plaintext block to ciphertext block
- “Substitution Cipher”

Stream Cipher

- Encrypted 1 symbol at a time
- Combined with a ***Stream*** of key material (key stream)

Monoalphabetic Substitution (Caesar cipher)

Each letter of plaintext maps to exactly one cipher symbol

(Block Size: 1 letter)

Let’s race! Decrypt the following:

RYG WKXI CSLVSXQC NY IYE RKFO?

It’s a question, when you decrypt it, shout out the answer!

Caesar Cipher: “Shift” Cipher

Write out all letters and move them over (wrapping around)

A	B	C	D	E	F	…	X	Y	Z
X	Y	Z	A	B	C	…	U	V	W

KEY SPACE: How many keys are there for this algorithm?

Permutation Cipher

Any letter can be mapped to any letter:

A	B	C	D	E	F	G	H	I	J	K	L	M
X	N	B	Y	A	M	L	S	V	P	R	K	W

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	C	G	I	U	D	T	F	O	H	J	Q	E

Key space is now how big?

Block size is still 1

Key Space is related to exhaustive/brute-force search

- Even without a computer, a 25/26 key space is easy to brute force

Block Size is related to ***cryptanalysis*** e.g., frequency analysis

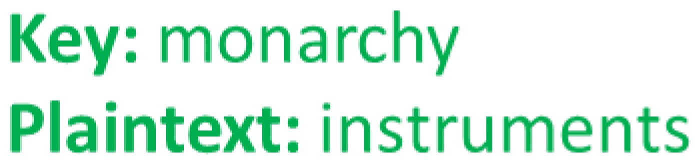
- A one-letter block does not conceal enough information

Playfair Cipher

1854 by Charles Wheatstone

Named after Lord Playfair who promoted it (classic politician)

Example: https://geeksforgeeks.org/playfair-cipher-with-examples



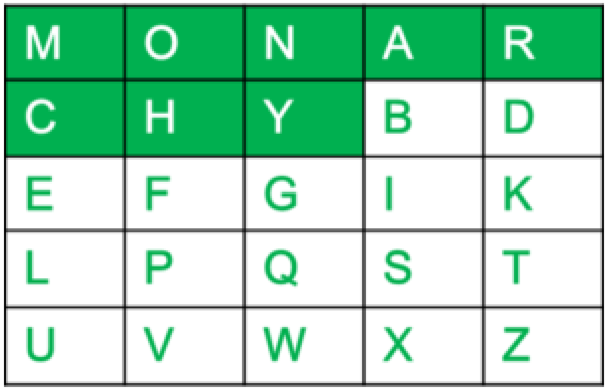
Key: monarchy
Plaintext: instruments

Playfair Keyblock

5×5 grid of alphabets that acts as the key (***Key Expansion***)

One letter of the alphabet (usually J) is omitted from the table

(If the plaintext contains J, then it is replaced by I)

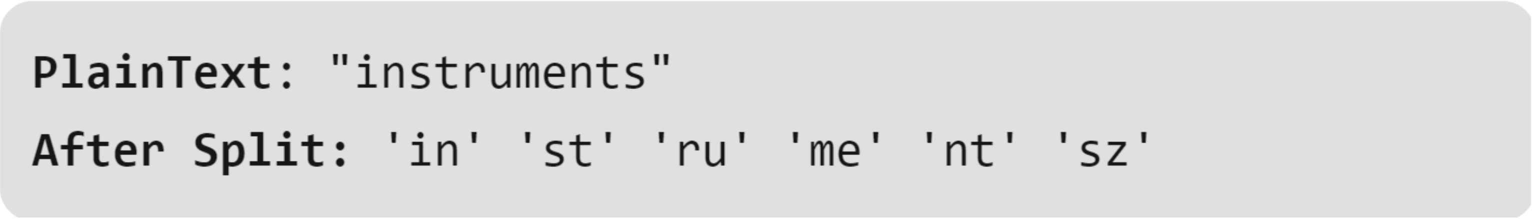


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Playfair Encipherment

The plaintext is split into pairs of two letters (digraphs).

If there is an odd number of letters, a Z is added to the last letter

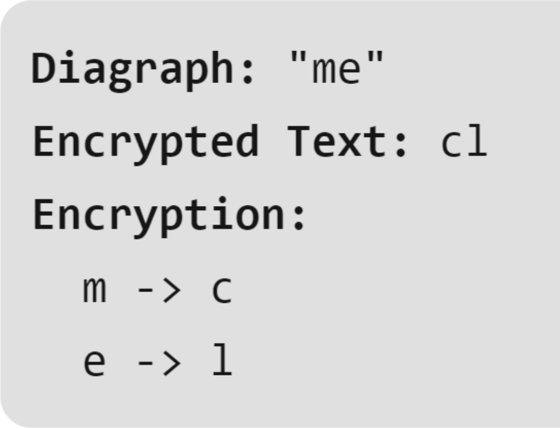


```
PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'
```

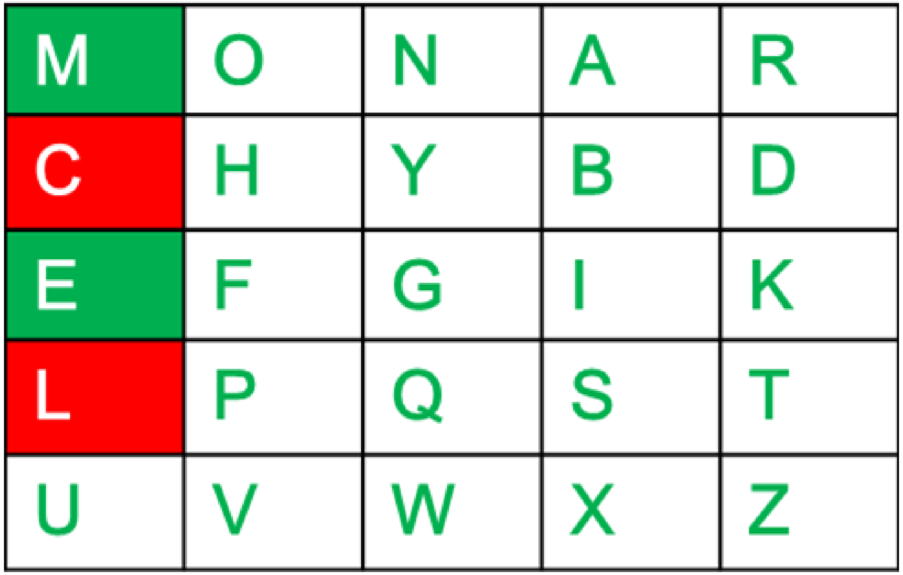
Playfair Encipherment

If both the letters are in the same column:

Take the letter below each one



```
Diagraph: "me"
Encrypted Text: cl
Encryption:
  m -> c
  e -> l
```



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Playfair Encipherment

If both the letters are in the same row:

Take the letter to the right of each one

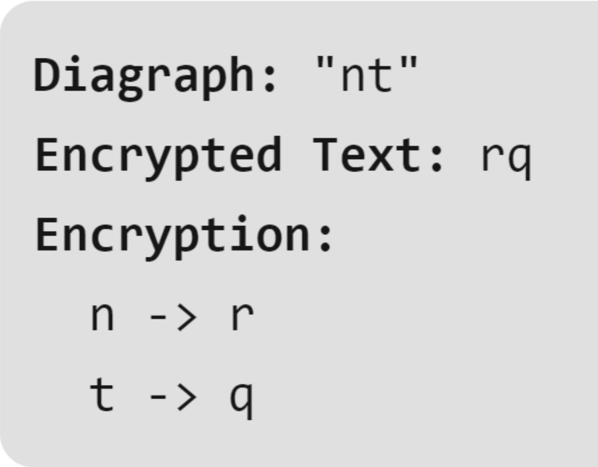
```
Diagraph: "st"
Encrypted Text: tl
Encryption:
  s -> t
  t -> l
```

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

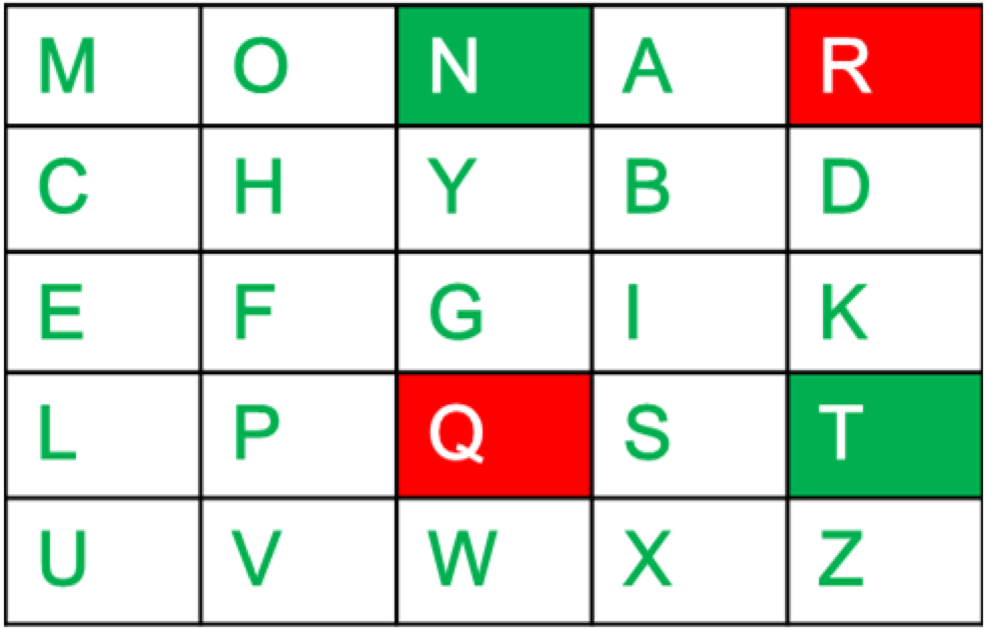
Playfair Encipherment

If letters do not share a row or column:

Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle



```
Diagraph: "nt"
Encrypted Text: rq
Encryption:
   n -> r
   t -> q
```



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Playfair Ciphertext:

Plain Text: "instrumentsz"

Encrypted Text: gatlmzclrqtx

How “Strong” is Playfair?

What’s the key space? How long to brute force?

What about “cryptanalysis”?

Cryptanalysis Considerations

Our example playfair ciphertext might be “uncrackable”

But what if the plaintext was longer?

How much ciphertext before **patterns** emerge?

Digraph (2-letter “blocks”) are better, but not good enough

Modern Requirements*

1. Symbols are just bits (can represent all info)
2. Blocks are large (used to be 64, now 128 bit)
3. Key size is large (currently 128 min, soon 256 bit min)
4. Algorithm has “Avalanche” property

*Not a formal list of all requirements; These are the ones that Dr. Nielson runs into most often

AES: Common Block Cipher

Block size is ***ALWAYS*** 128 bits

Key size can be 128, 192, or 256

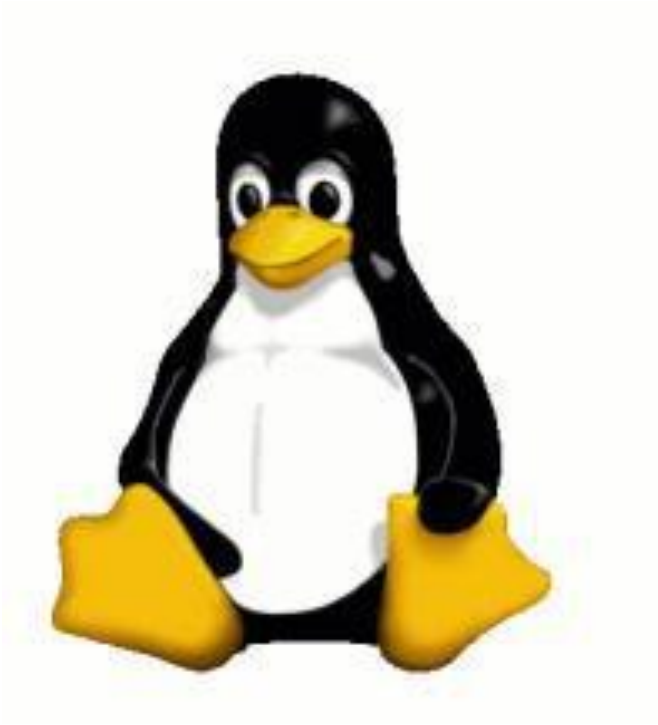
But at its core, still a “substitution” cipher.

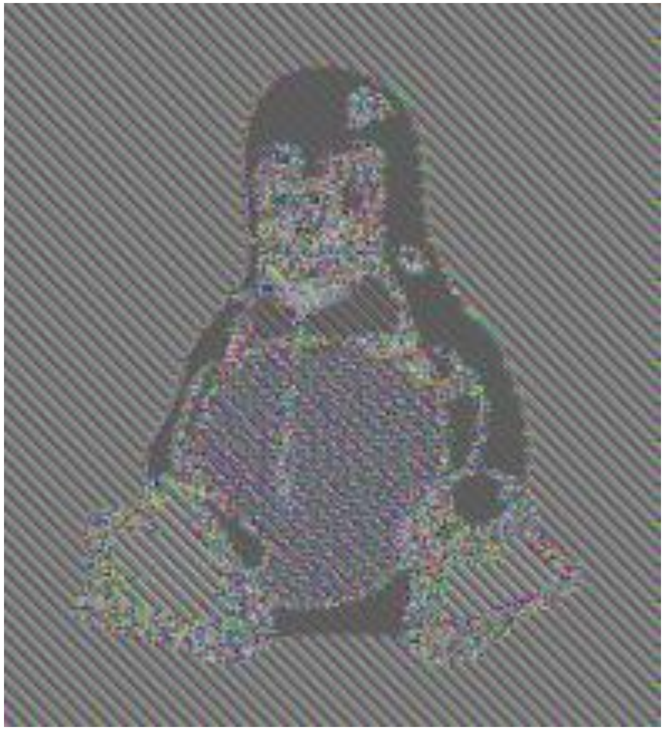
AES-128 encryption of ”My name is Seth!” w/ a “zero” key:

E94B 69E7 13C6 B4F9 B834 FEA5 95F7 8F2A

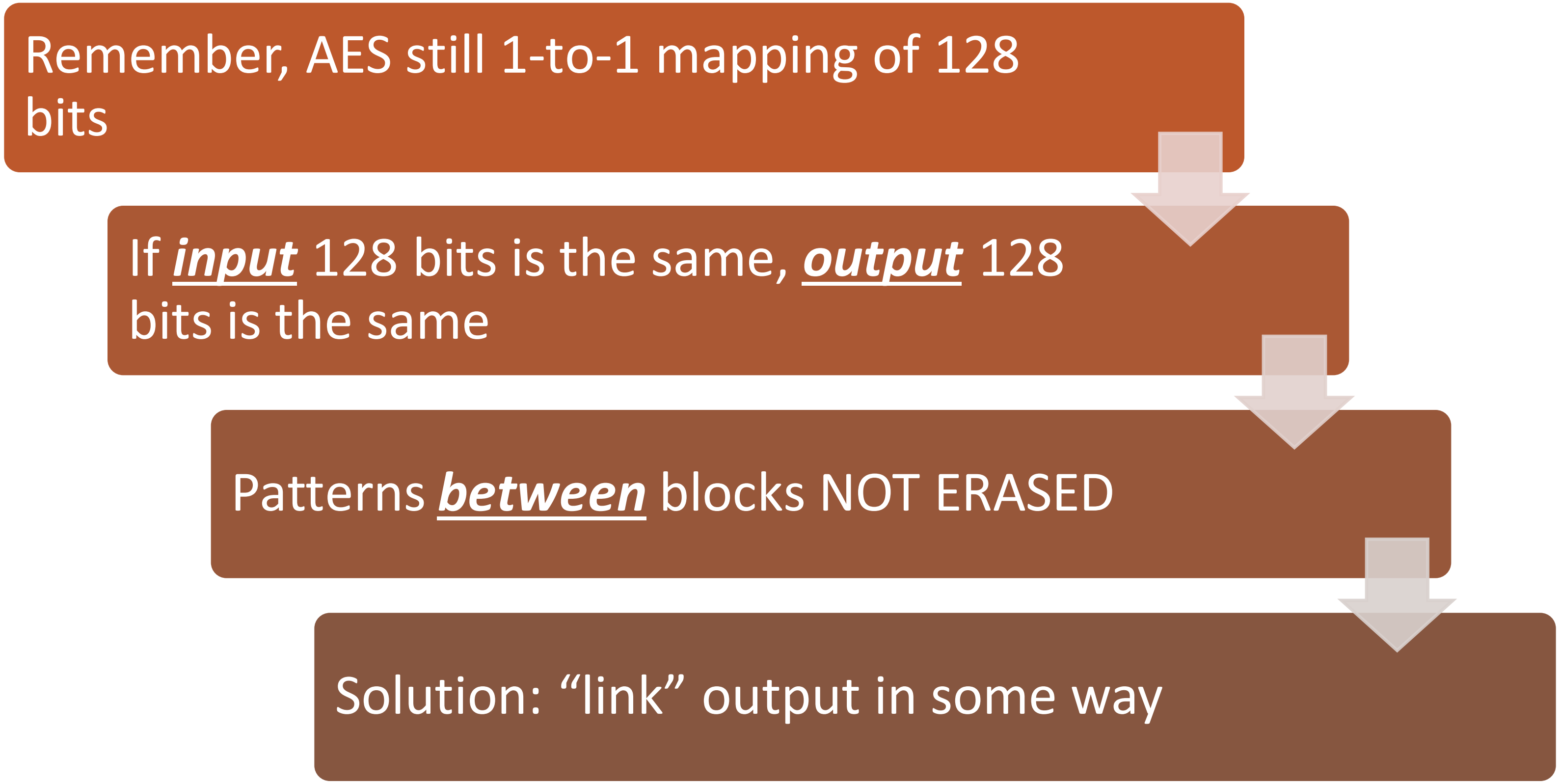
Block Cipher Weaknesses

What happened here?





Patterns



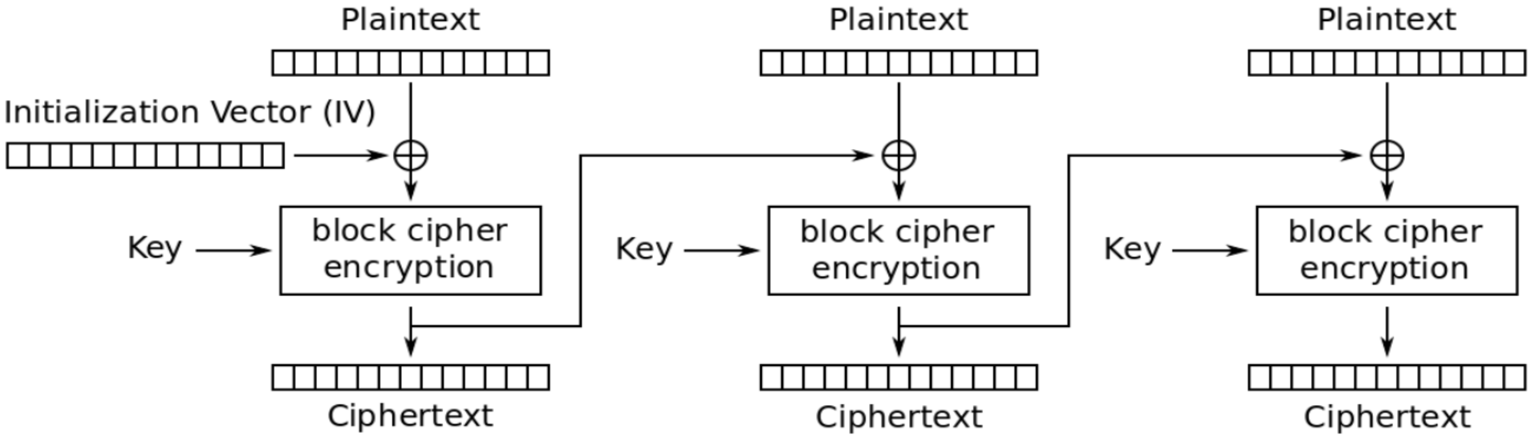
Remember, AES still 1-to-1 mapping of 128 bits

If ***input*** 128 bits is the same, ***output*** 128 bits is the same

Patterns ***between*** blocks NOT ERASED

Solution: “link” output in some way

Cipher-Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

What is an IV?

Initialization Vector

Similar to “salting” a hash

Eliminates deterministic output

You should almost never reuse a key

BUT YOU SHOULD NEVER EVER reuse a KEY and IV

Quasi-Deprecated CBC

CBC “works” ***when used correctly***

However, has various weaknesses and is error prone

In many cases, CBC is being deprecated

Counter Mode (CTR)

Converts a block cipher into a ***STREAM CIPHER***

Does NOT encrypt the plaintext directly

Rather, is used to generate a key stream

Keystream = AES(IV + 0), AES(IV + 1), AES(IV + 2)…

Ciphertext = Plaintext XOR Keystream

Plaintext = Ciphertext XOR Keystream

Don’t Reuse Keystream

C1 = K1 xor M1

C2 = K1 xor M2

C1 xor C2 = K1 xor M1 xor K1 xor M2

= K1 xor K1 xor M1 xor M2

= M1 xor M2

Confidentiality does NOT provide Integrity

Start with a ciphertext   C1 = K XOR M1

Suppose an attacker knows the plaintext M1 (or part of it!)

Suppose attacker can intercept/change the message

Attackers wants to change M1 to M2

Attacker produces C2 = C1 xor (M1 xor M2)

= K xor M1 xor M1 xor M2

= K xor M2

ALSO WORKS ON OTP (“provably secure”)

Integrity in History

Message integrity also pre-dates modern cryptography

Bank transfers in the 19th century used the telegraph

How to keep a telegraph operator from sending a false message?

Banks developed code but this did nothing for *message integrity*

Banks developed code books with a “test key”

- The test key had one-way calculations for money, dates, currency, etc
- The test key computed and the test key transmitted had to match
- Not great by today’s standards, but worked until the 1980’s!!!

Modern Hashing

1. Compression
2. Ease of Computation
3. Preimage Resistance
4. 2nd Preimage Resistance
5. Collision Resistance

In practice, also has the Avalanche property

Message Authentication Code

MAC is a symmetric key code that is used for message integrity

Commonly implemented as a ***keyed*** hash

Super simple MAC: hash(message + key)

HMAC is more complicated, but same basic idea:

HMAC_k(M) = h(k xor A, h(k xor B, M))

- A = repeated 0x36
- B = repeated 0x5c

Composite Mode

Also known as

- Authenticated Encryption or
- **AEAD – Authenticated Encryption with Additional Data**

Integrity + Confidentiality

AES-GCM is counter mode with a built-in MAC (called a “tag”)

AES-CCM is counter mode with CBC-MAC

Only AEAD ciphers supported in TLS 1.3

TAKEAWAY MESSAGE: **USE AEAD WHENEVER POSSIBLE!!!!!!!!**