Cryptography in Network Security

UT CS361S

SPRING 2021

LECTURE NOTES

This is NOT a Crypto Course

This course: ***Network Security***

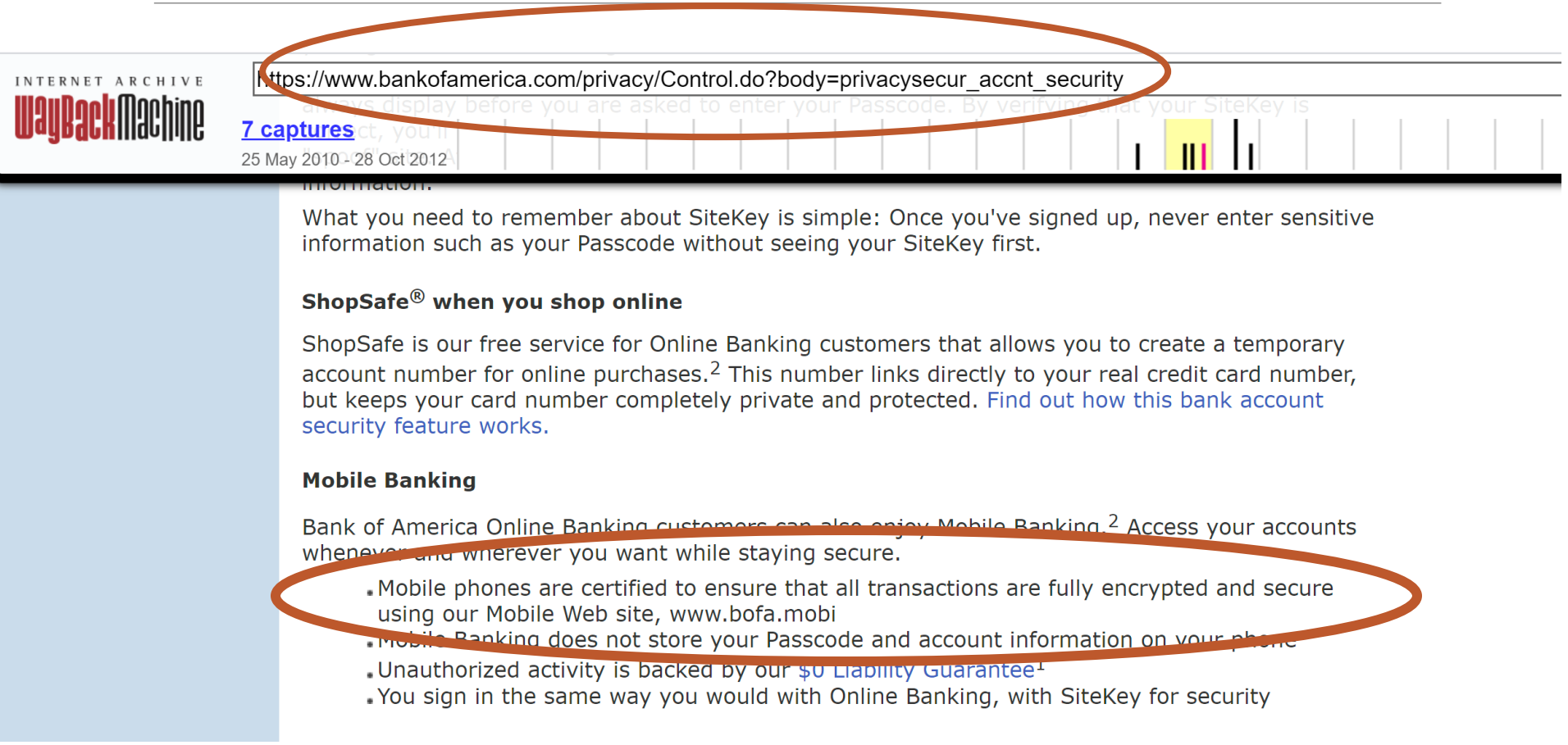
Network Security ≠ Cryptography

But, ***crypto is used extensively in network security***

We will discuss some basic crypto concepts

But mostly, we will see how crypto is used to secure networks

What is “Cryptography”?



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

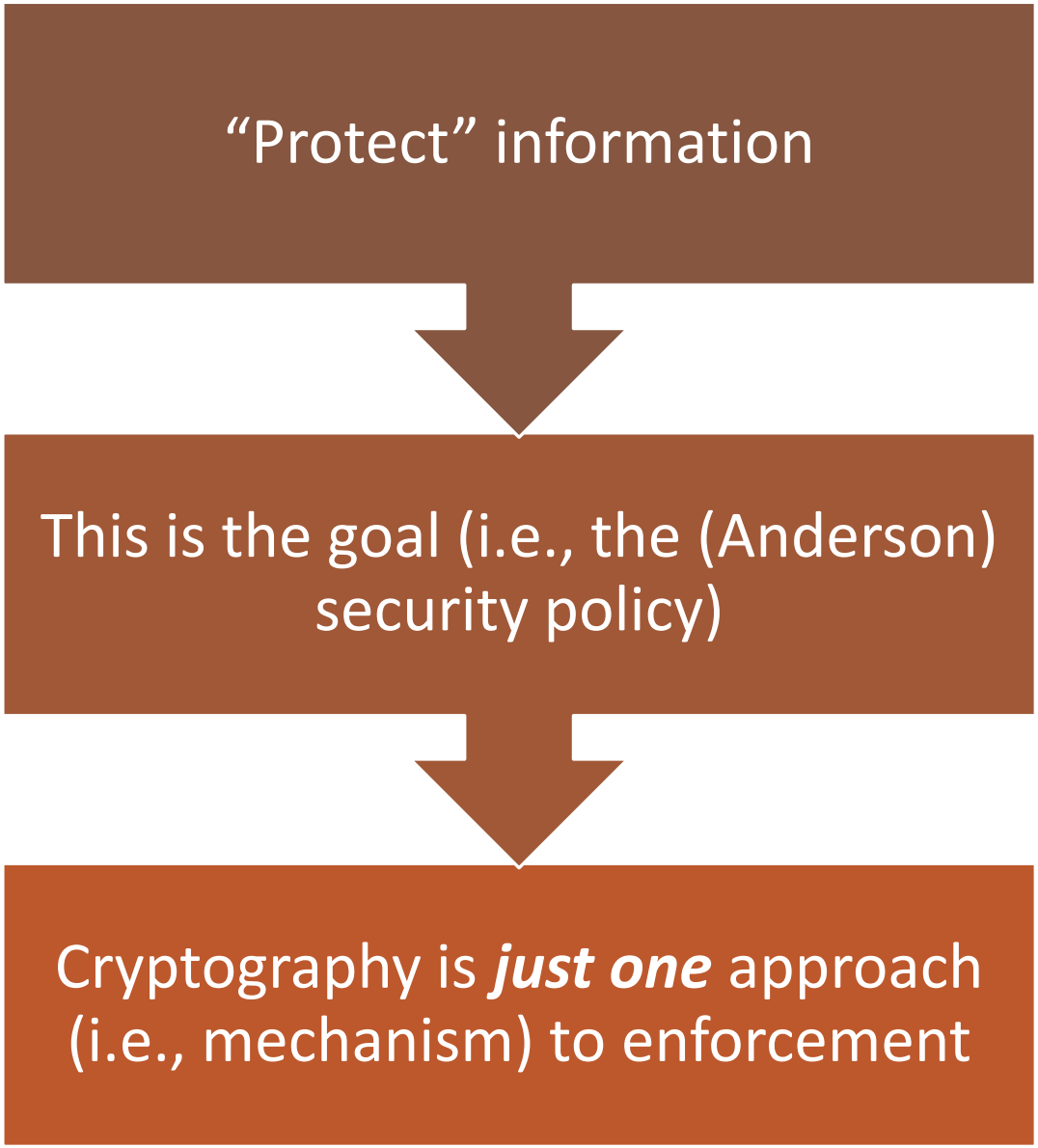
Assume definition of “information” is axiomatic

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



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.

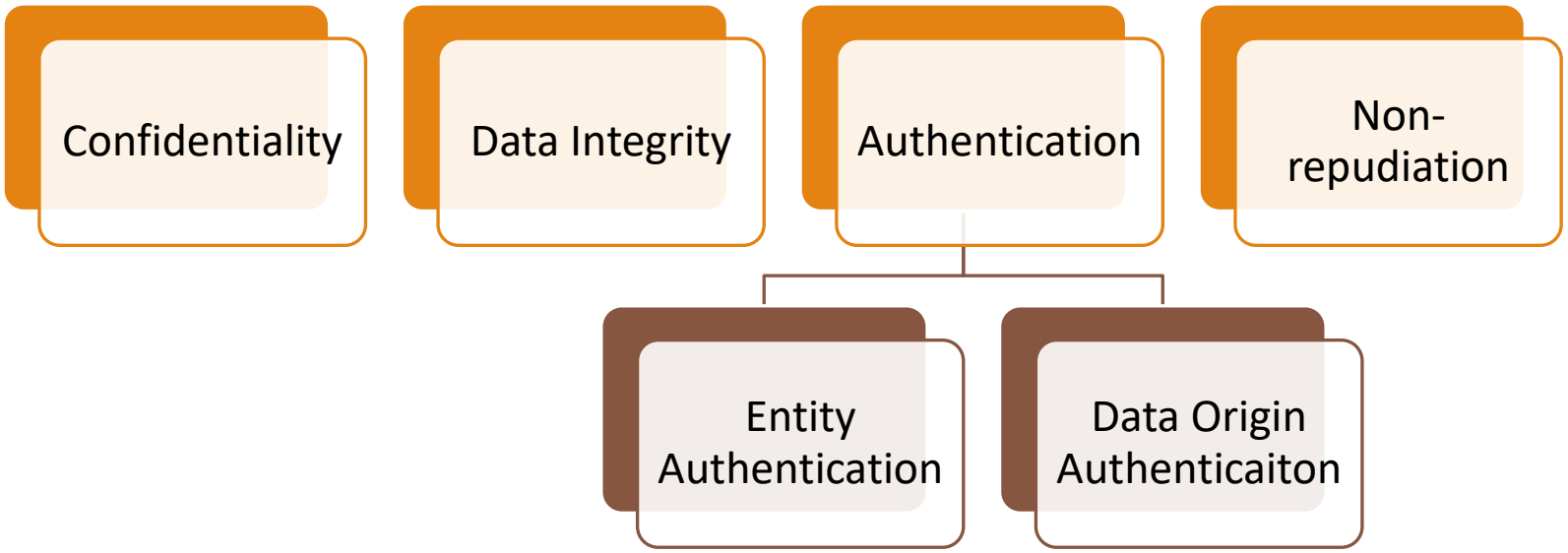
Information Security Objectives

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

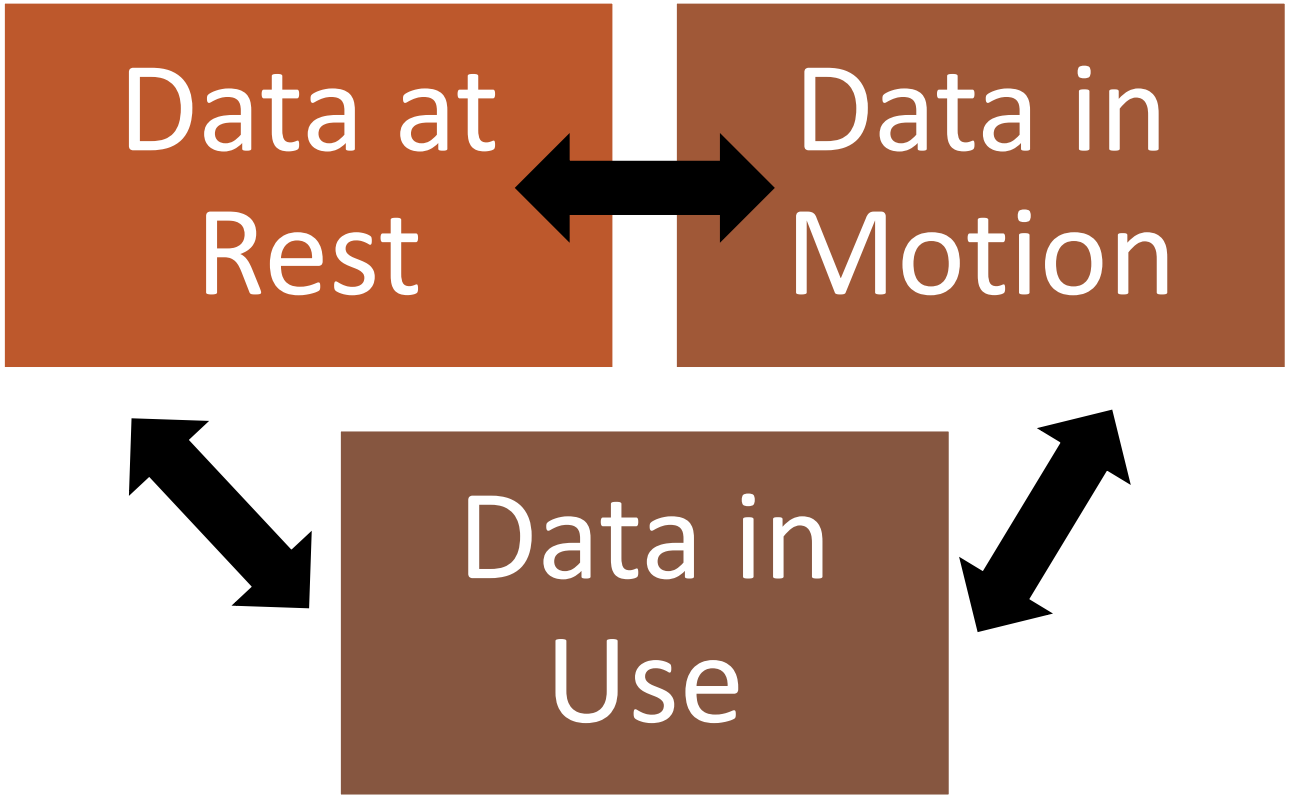
receipt	acknowledgement that information has been received.
confirmation	acknowledgement that services have been provided.
ownership	a means to provide an entity with the legal right to use or transfer a resource to others.
anonymity	concealing the identity of an entity involved in some process.
non-repudiation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

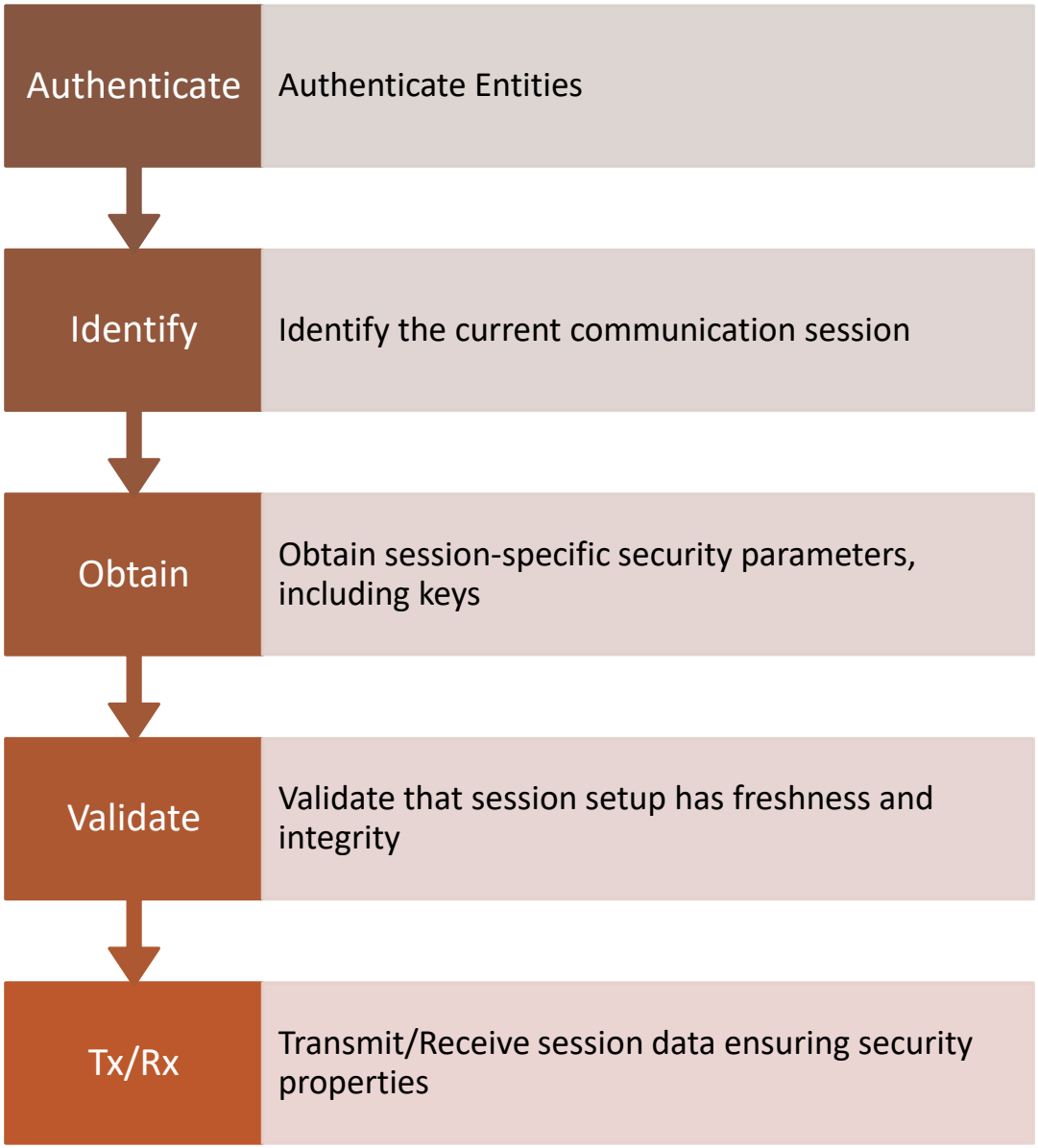
- Common objective: Over-the-network entity authentication
- Common objective: Secure Authenticated Channel

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!)

EXAMPLE
Secure Authenticated Channels



Cryptographic “Primitives”

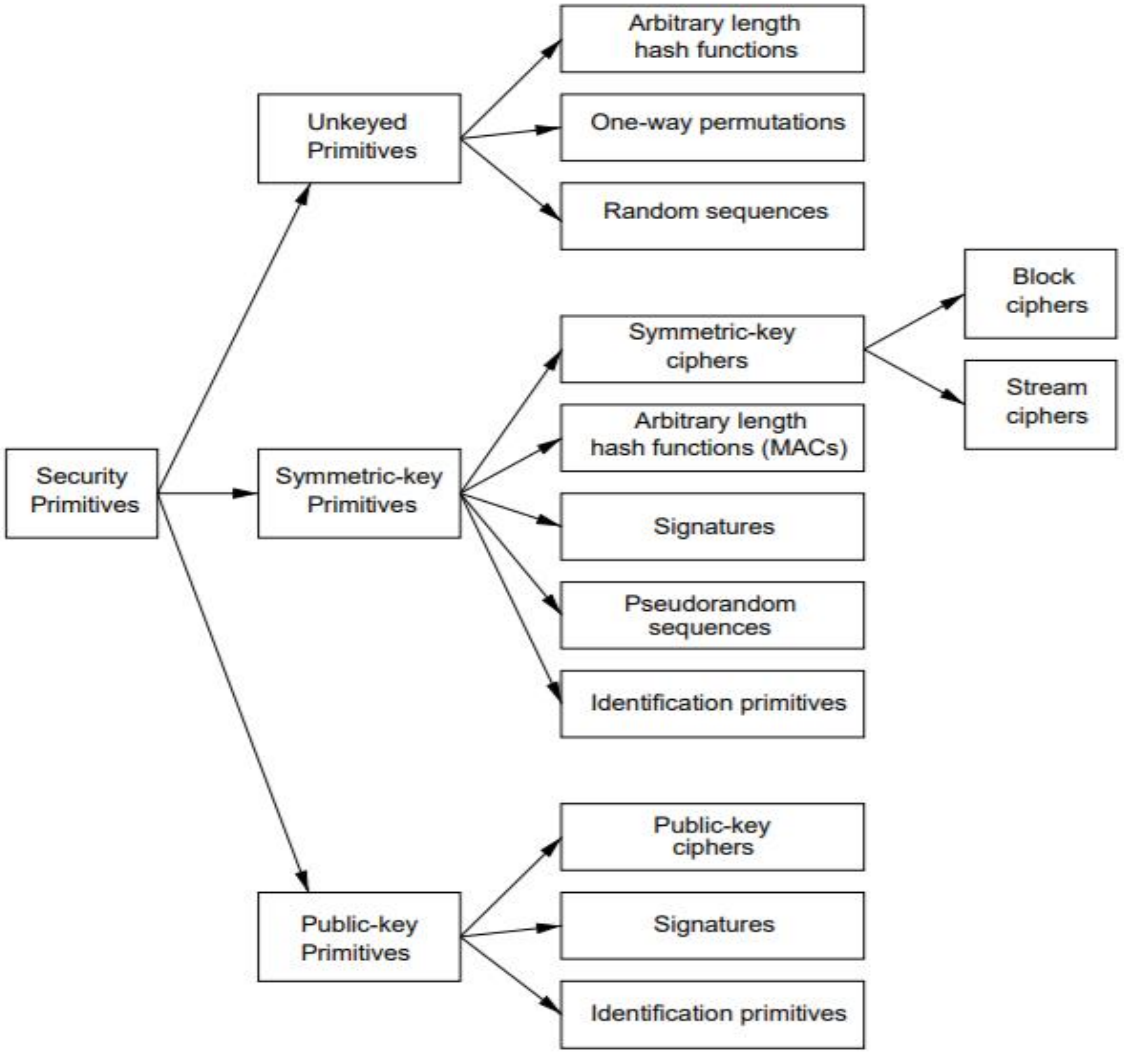


Figure 1.1: *A taxonomy of cryptographic primitives.*

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 <u>more</u> dangerous, not less!***

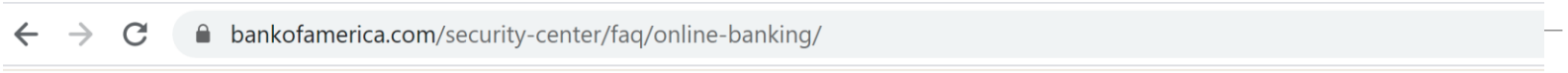
Do NOT roll your own cryptography

Know when to tell your boss to hire a cryptography expert

My Objective

1. Students are conversant about basic cryptography terms and vocab
2. Students can recognize/understand cryptographic errors/failures
3. Students understand how crypto can enforce policy
4. Students can recognize mismatches in policy/enforcement
5. Students understand the crypto in common network protocols
6. Students know when to seek out subject-matter experts

Improvement!



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.