Theory and Practice of Cryptography

From Classical to Modern

About this Course

All course materials: http://saweis.net/crypto.shtml

Four Lectures:

1. History and foundations of modern cryptography.
2. Using cryptography in practice and at Google.
3. Theory of cryptography: proofs and definitions.
4. A special topic in cryptography.

Classic Definition of Cryptography

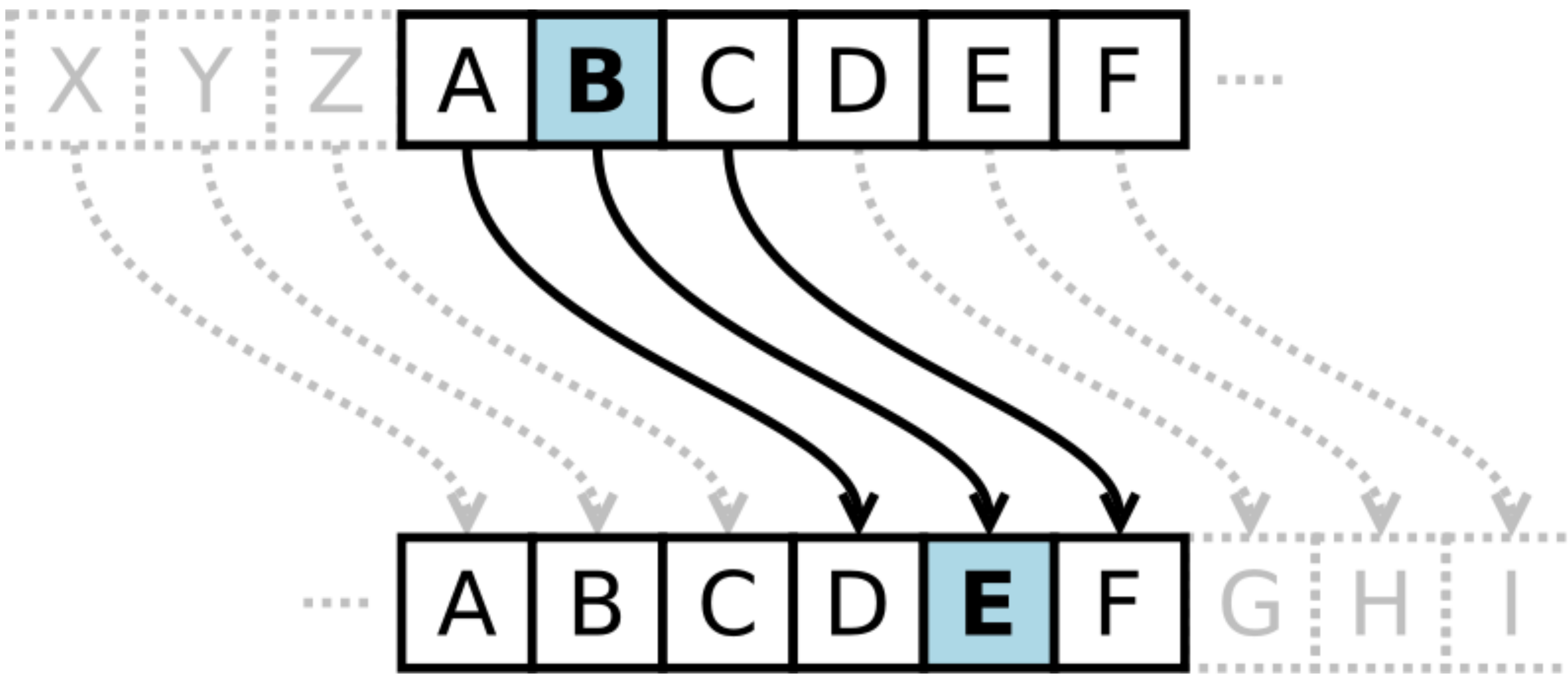
Kryptósgráfo , or the art of "hidden writing", classically meant hiding the contents or existence of messages from an adversary.

Informally, *encryption* renders the contents of a message unintelligible to anyone not possessing some secret information.

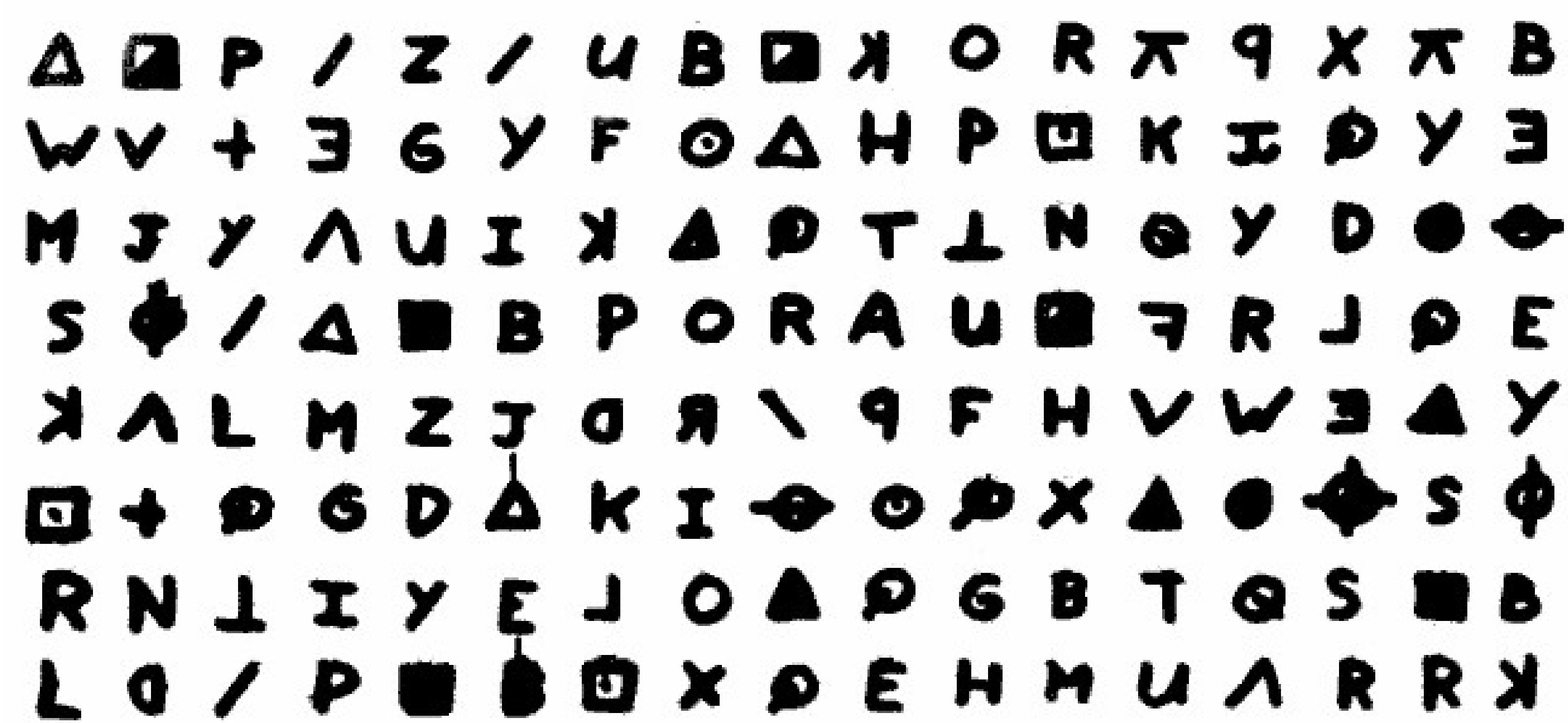
Steganography, or "covered writing", is concerned with hiding the existence of a message -- often in plain sight.

Scytale Transposition Cipher

Caesar Substitution Cipher



Zodiac Cipher

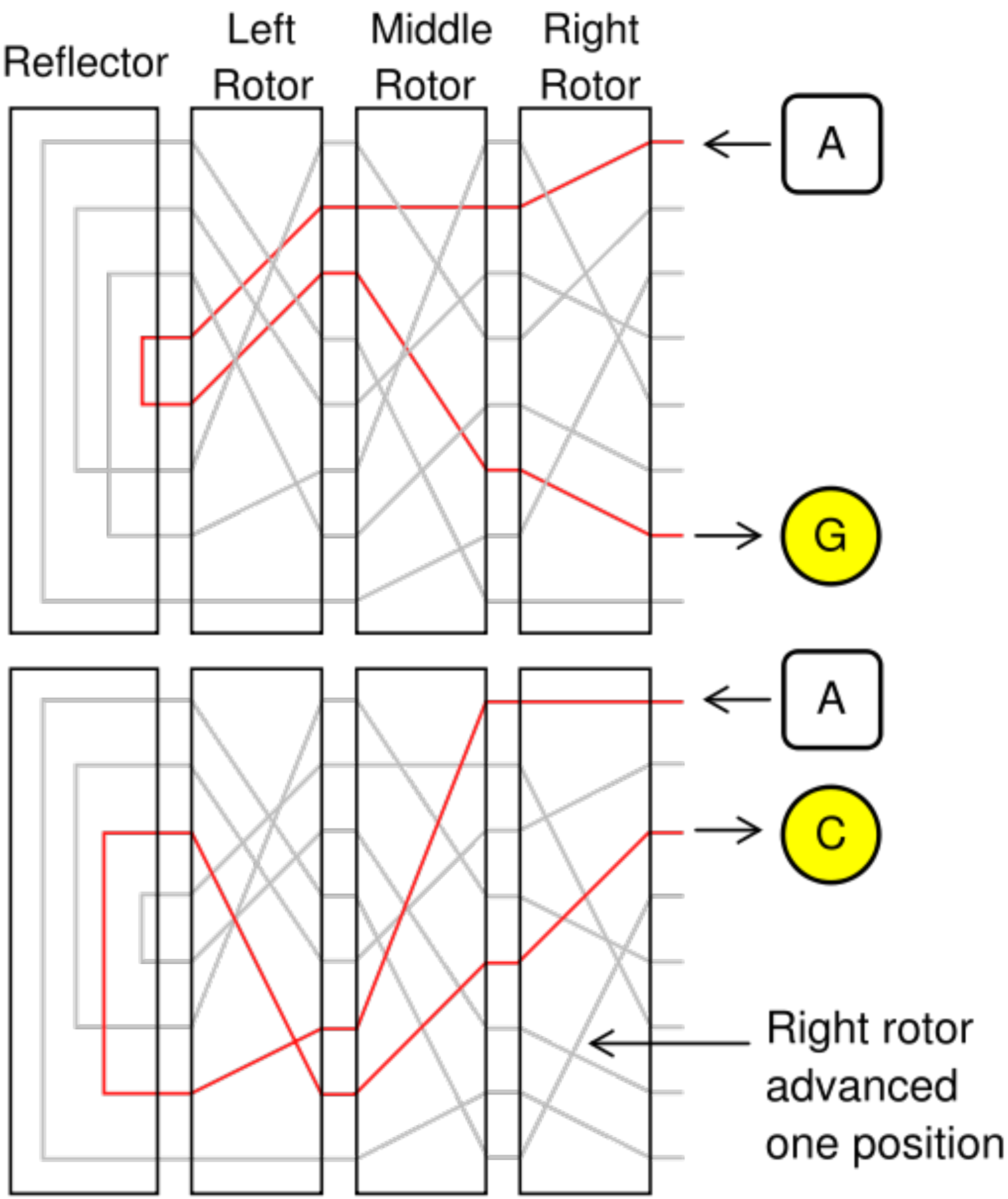


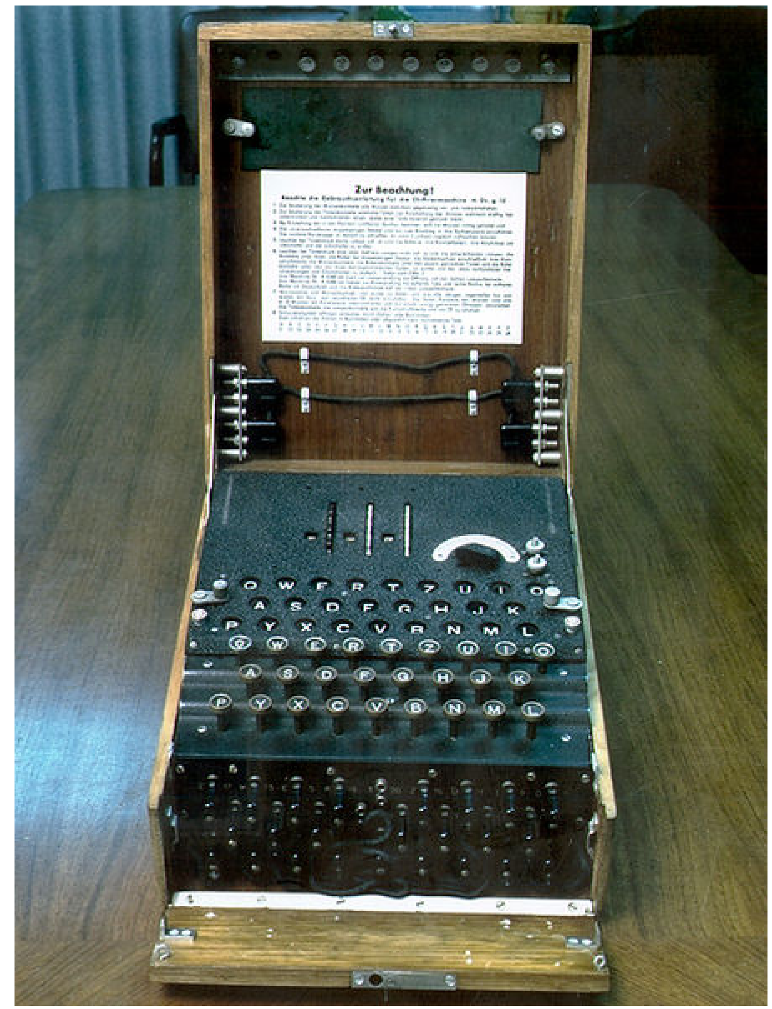
Vigenère Polyalphabetic Substitution

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

Key:
GOOGLE
Plaintext:
BUYYOUTUBE
Ciphertext:
HIMEZYZIPK

Rotor-based Polyalphabetic Ciphers





Steganography

- Herodotus tattoo and wax tablets
- Invisible ink
- Microdots
- "The Finger"
- Prison gang codes
- Low-order bits

Codes

Codes replace a specific piece of plaintext with a predefined code word. Codes are essentially a substitution cipher, but can replace strings of symbols rather than just individual symbols.

Examples:

- "One if by land, two if by sea."
- Beale code
- Numbers stations
- ECB Mode

Kerckhoffs' Principle

A cryptosystem should be secure even if everything about it is public knowledge except the secret key.

Do not rely on "security through obscurity".

One-Time Pads

Generate a random key of equal length to your message, then exclusive-or (XOR) the key with your message.

This is information theoretically secure...but:

- "To transmit a large secret message, first transmit a large secret message"
- One time means one time.
- Need to transmit a key per message per recipient.
- Keys are as big as messages.

Problems with Classical Crypto

Weak: Pen and paper, and mechanical cryptosystems became weak in the face of modern computers.

.

Informal: Constructions were ad hoc. There weren't publicly available security definitions or proofs of security.

Closed: Cryptographic knowledge and technology was primarily only available to military or intelligence agencies.

Key distribution: The number of keys in the system grows quadratically with the number of parties.

Modern Cryptographic Era

- Standardization of cryptographic primitives
- Invention of public key cryptography
- Formalization of security definitions
- Growth of computing and the internet
- Liberalization of cryptographic restrictions

Government Standardization

- Data Encryption Standard (DES): A strong, standardized 56-bit cipher designed for modern computers

- Originally designed by IBM and called "Lucifer". Tweaked by the NSA and published in 1975.

- In 1999, a DES key was brute forced in 24 hours for $100K
- Triple DES (3DES): Effectively 112-bit cipher. Still in use.

- Advanced Encryption Standard (AES) is modern heir to DES, and was designed by academics in a public competition.

- AES supports 128-bit and larger keys.

Key Distribution Problem

- How do Alice and Bob first agree on a shared key?
- What happens if either party is compromised?
- What happens when Carol wants to talk to Alice and Bob?

Diffie-Hellman Key Exchange

Diffie-Hellman-Merkle (1976) / Williamson (1974):
Generate a shared secret with a stranger over a public channel.

1. Alice picks a group G, generator g, and a random value x
2. Alice computes A = g^x and sends Bob (G, g, A)
3. Bob picks a random y, computes B = gy, and sends Alice B
4. Alice computes K = B^x = g^(xy)
5. Bob computes K = A^y = g^(xy)

Eve's sees (G, g, A, B) = (G, g, g^x, g^y)
How hard is it for her to compute g^(xy)?

Note: "^" is the power operator, not an XOR

Diffie-Hellman Key Exchange

Does this solve the key distribution problem? Not quite..

- Still need to establish n^2 keys for n people or conduct interactive key exchange protocols for each message.

- Computation over appropriate groups can be expensive

- Vulnerable to a man in the middle attack

Public Key Encryption

What if you could publish a "public" key that anyone could use to encrypt, but not decrypt messages?

1. A public key cryptosystem consists of (G, E, D).
2. Alice generates a *key pair:* $G(r) \rightarrow (PK_a, SK_a)$
3. Alice publishes her public key PK_a
4. Bob encrypts a message with her public key: $E(PK_a, m) \rightarrow c$
5. Alice decrypts a ciphertext with her secret key: $D(SK_a, c) \rightarrow m$

Public Key Encryption

Nice properties:

- Only one key per person, not per pair.
- Can communicate with a stranger without agreeing on a key.

Problems with public key cryptography:

- Is this even possible?
- How do you get Alice's public key?
- Why do you trust the ciphertext?

RSA Encryption

Published in 1977 / Cocks 1973

Based on hardness of factoring products of large primes.

1. Setup: $n = pq$, $PK = (e, n)$, $SK = d$, $ed = 1 \bmod (p-1)(q-1)$
2. $E(PK, m) = m^e \pmod{n} = c$
3. $D(SK, c) = c^d \pmod{n} = m^{(ed)} \pmod{n} = m$

Problems?

- Ciphertext is fixed size
- Computation is still relatively expensive.
- Why do you trust the ciphertext has not been modified?
- Not *semantically secure* (lecture 3)

What about authentication?

- How do we know Alice is Alice?
- How do we know a message originated from Alice?
- How do we know Alice's message was not altered in transit?

Message Authentication Codes

- Alice and Bob share a secret key k.
- Either can sign (or MAC) a message: Sign(k, m)$\rightarrow$ σ
- The recipient can verify the signature: Verify(k, m, σ)
- Often built from other primitives
- Similar key distribution problems to ciphers

Public Key Signatures

Only you can sign messages, but anyone in the world can verify them. Public-key analog of a MAC.

1. A public key signature scheme consists of (G, Sign, Ver).
2. Alice generates a *key pair:* $G(r) \rightarrow (VK_a, SK_a)$
3. Alice publishes her verifying key VK_a
4. Alice signs a message: $Sign(SK_a, m) \rightarrow \sigma$
5. Bob verifies a signature with her verifying key: $Ver(VK_a, m)$

Public Key Signatures

- Is a public key signature scheme possible?
- How do we distribute verification keys?
- RSA is fixed size. How do we sign big messages?

Message Digests

- Message digests compress input to fixed length strings.
- No keys involved.
- <u>One-wayness:</u> It is hard to find an input that hashes to a pre-specified value.
- <u>Collision resistance:</u> Finding any two inputs having the same hash-value is difficult.
- Fixed-length public signature schemes can sign digests instead of the actual message.

Key Distribution: Still a problem

How do you know someone's public key is their own?

- Certificates: A signature on a public key or another certificate

- PKI: A graph of relationships between keys.
  - Certificate authorities
  - A "web-of-trust" social graph

How do we revoke keys?

- Expiration dates

- Certificate Revocation Lists

The Rest of the Course

Exercise Set 1: Posted on http://go/cryptocourse

Lecture 2: Using cryptography in practice. Engineering-oriented

Lecture 3: Theory of cryptography. Math-oriented.

Lecture 4: A special crypto topic. General audience.