Digital Signatures

Kara Breeden and Aviva Kosansky

What is a Digital Signature

Digital = consisting of a string of digits

PARADOXICAL!

Strings of digits can be copied but signatures are not meant to be copied.

https://www.chmag.in/wp-content/uploads/2012/09/
electronic-signature.jpg

What are Digital Signatures?

- Material that requires verification
    - Usually when the material is being sent to you instead of you sending the material
- Most well known: Software Signing
    - Valid signatures will tell you the maker of some software and can give the user comfort
    - No signature means no information and this can be potentially dangerous
    - Websites with https send a digitally signed certificate before establishing a secure connection
- Signing your name as a signature
    - Where an online form asks for name
    - This is not what we want you to think of! Why not?

Paper Signatures

Signature Bank

Used to compare a person’s paper signature to itself to make sure it is valid

Trust the source that the signature is correct

Problems with Paper Signatures:

Easy to obtain and

http://www.fdpexpert.com/images/bigstock-Contract-with-person-signing-n-26173646_-_Copy.jpg

Signing with a Padlock

Lock and Keys

- Owned by one person, both locks and keys
- The owner is the ONLY one who can lock the lock
- The owner must physically give someone the key to unlock the lock
- Anyone with a key can unlock the lock

http://www.globalnerdy.com/wordpress/wp-content/uploads/2014/07/unlocked-padlock-with-key.jpg

Lock IS signatu

- Generally nee k is the signature
  - Ex: In a third party that would store the keys for the lock

Signing with a Multiplicative Padlock

Physical → Numerical

Padlocks and Keys are represented by numbers

Locking and Unlocking are represented by multiplication in clock arithmetic

Message passed is a sequence of a string of numbers

Multiplicative Padlock Trick

Message = Number

Padlock = Different number

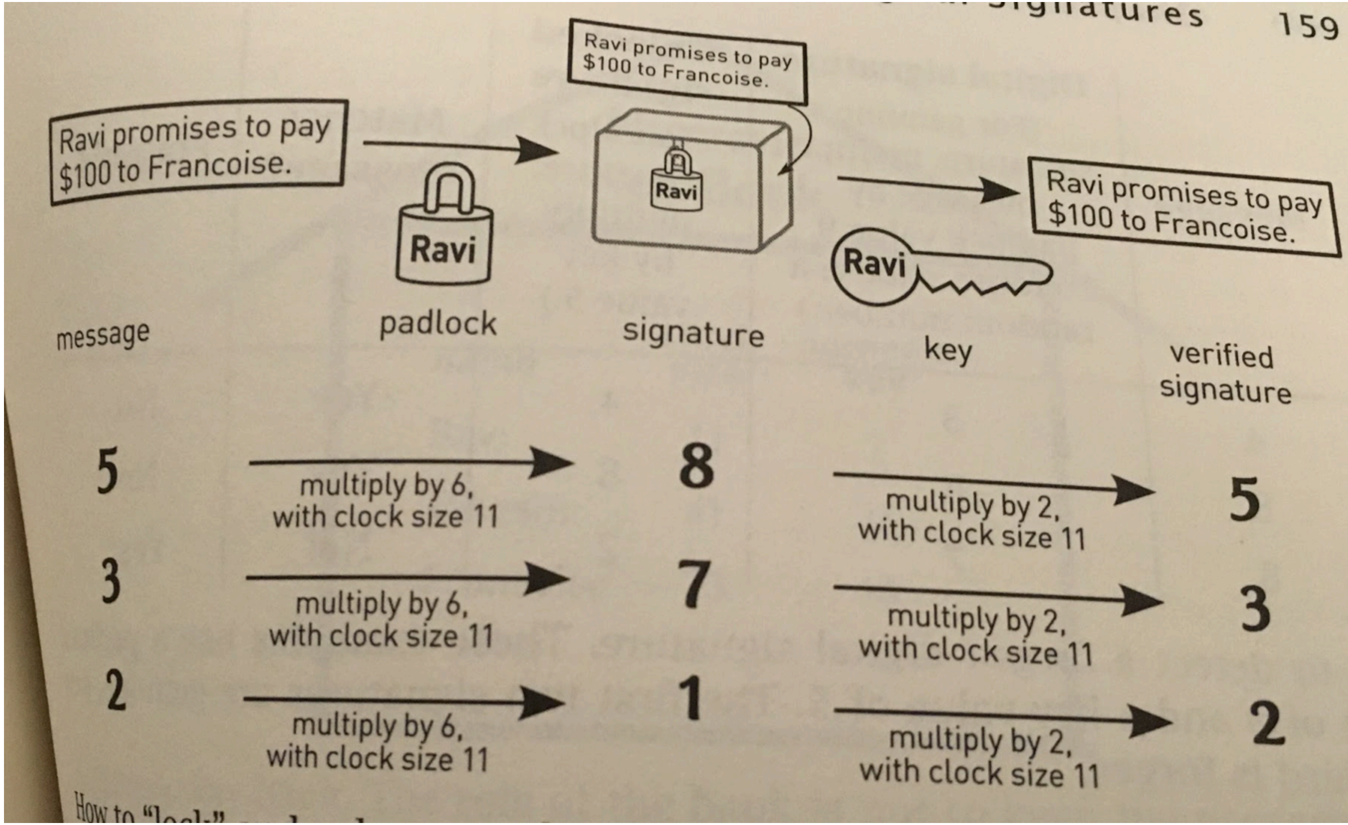
Owner chooses clock size and number to represent the padlock

Result = Message x Padlock (using multiplication in clock arithmetic)

Result = Digital signature for original message

Key = number selected to unlock previously chosen padlock number

Verify Signature = Key x Result (using multiplication in clock arithmetic)


Ravi promises to pay
$100 to Francoise.
Ravi
Ravi promises to pay
$100 to Francoise.
Ravi
Ravi
Ravi promises to pay
$100 to Francoise.
message
padlock
signature
key
verified
signature
5
multiply by 6,
with clock size 11
8
multiply by 2,
with clock size 11
5
3
multiply by 6,
with clock size 11
7
multiply by 2,
with clock size 11
3
2
multiply by 6,
with clock size 11
1
multiply by 2,
with clock size 11
2

How to “lock”

Padlock Trick cont.

Padlock number MUST be secret

Can reveal message number, signature, key value and clock size

Still need third party

- Without third party
  - the owner can give false key
  - Others can make padlock and key and say it is the owners

In Short:

Numeric Padlock : PRIVATE

How Numbers are Chosen

Clock size is any prime number

Padlock is any positive number smaller than clock size

Key is generated by a computer using Euclid’s algorithm

Flaw: Computer given key value can generate padlock number by applying the algorithm again

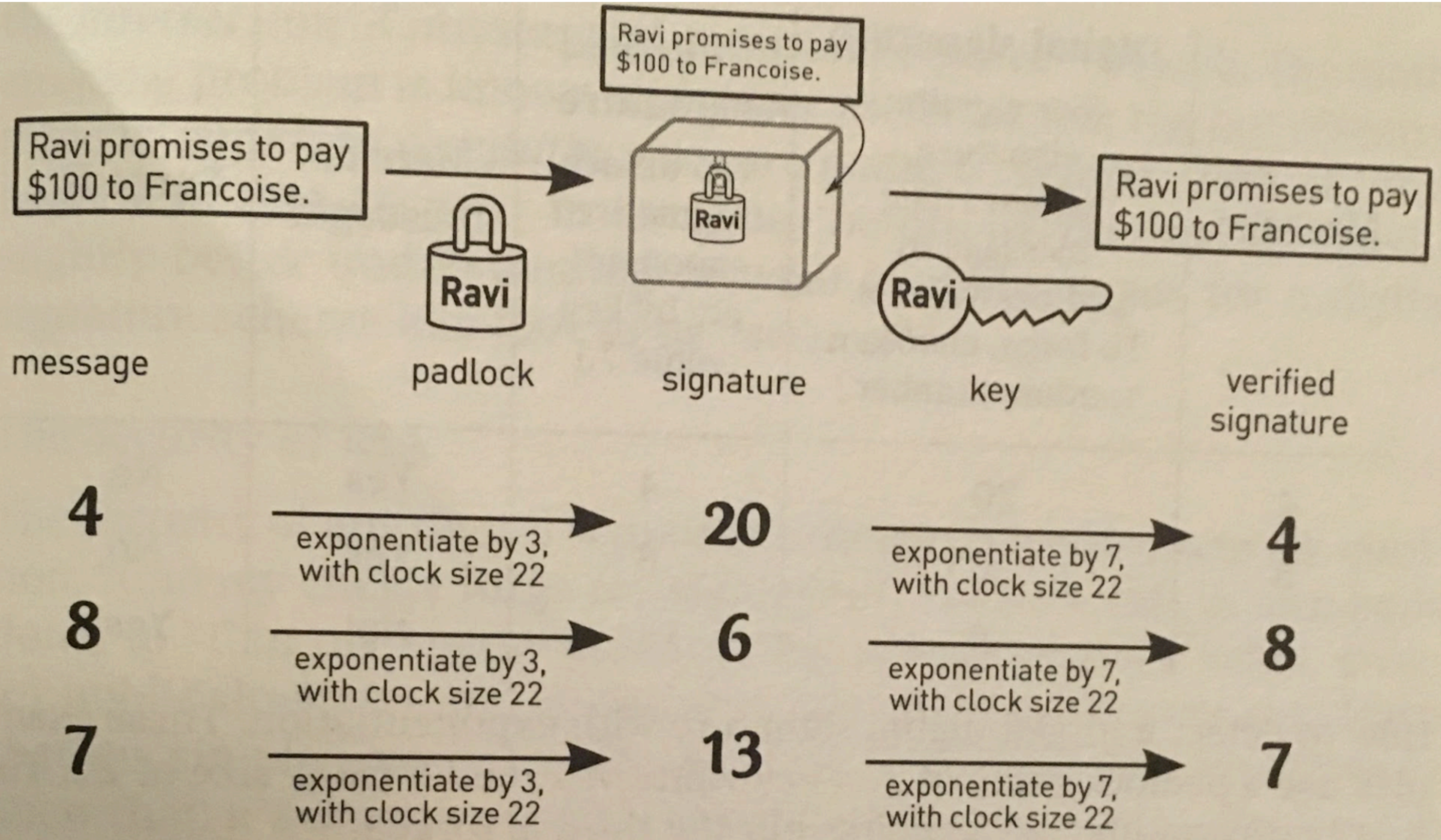
Don’t use multiplication -- Don’t use this approach

Exponent Padlock

Known as RSA and is the approach used for digital signatures

- Same approach as multiplicative technique but using exponentiation
    - Message = Base
    - Padlock = Exponent
    - Signature = result of exponentiation with clock arithmetic

- User picks padlock (any number < clock size) and clock size (any number)
- Key is computed by computer


Ravi promises to pay $100 to Francoise.
Ravi promises to pay $100 to Francoise.
Ravi
Ravi
Ravi
Ravi promises to pay $100 to Francoise.
message
padlock
signature
key
verified signature
4
exponentiate by 3, with clock size 22
20
exponentiate by 7, with clock size 22
4
8
exponentiate by 3, with clock size 22
6
exponentiate by 7, with clock size 22
8
7
exponentiate by 3, with clock size 22
13
exponentiate by 7, with clock size 22
7

Locking and unlocking messages using exponentiation.

RSA System

RSA is both Public Key Cryptography Scheme AND Digital Signature Scheme

Person can compute key easily based off of padlock but it is impossible to reverse the process even if you know the clock size

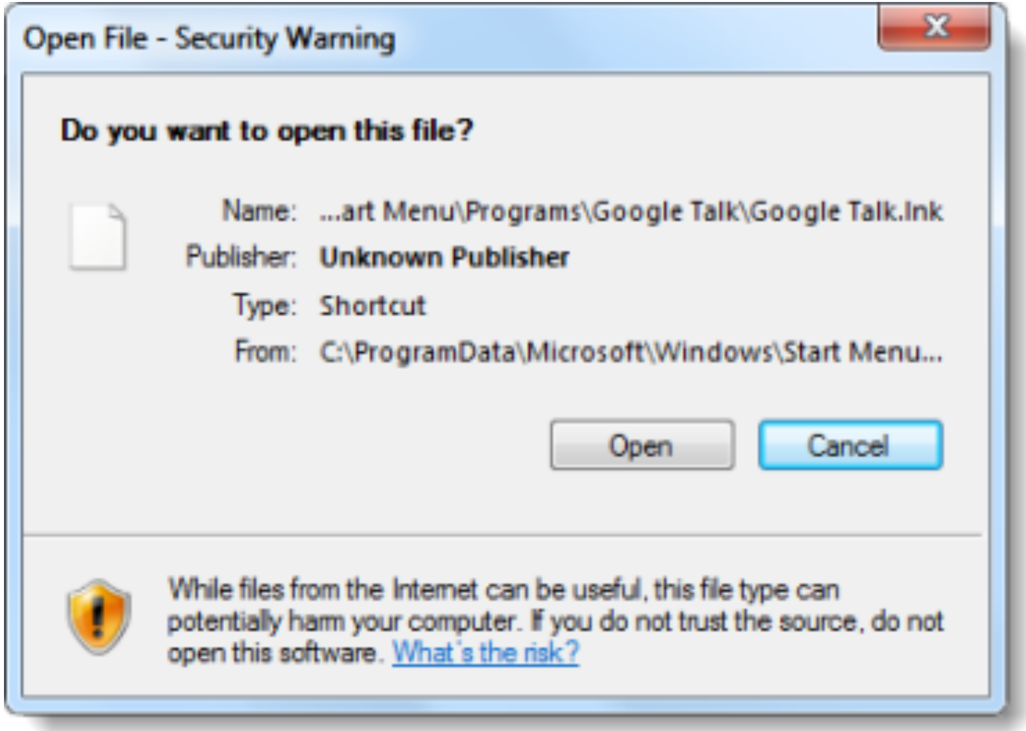
Has not been proven and so the algorithm is considered to be secure for now

To generate clock size for RSA you multiply two prime number together

Brakes: if clock size is factorized into 2 prime numbers (key can easily be reversed)

People try to crack it and there is no efficient way even with Quantum computers

Digital Signatures in Practice



Open File - Security Warning

Do you want to open this file?

Name: ...art Menu\Programs\Google Talk\Google Talk.lnk

Publisher: **Unknown Publisher**

Type: Shortcut

From: C:\ProgramData\Microsoft\Windows\Start Menu...

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Certification Authority

Maintain servers that are contacted electronically to download public key information

When the computer gets a signature it comes with information stating which CA can vouch for the signer's public key

CA = THIRD PARTY
How do we trust third party?

http://www.groovypost.com/wp-content/uploads/2010/10/image36.png

Paradox Resolved

What do YOU think?

Summery

Without digital signatures the internet as we know it would not exist

No sources could be verified

Data could be transferred but not verified