Trust

• The “fabric” of life!
• Holds civilizations together
• Develops by a natural process
• Advancement of technology results in faster evolution of societies
  • Weakening the natural bonds of trust
  • From time to time artificial mechanisms need to be introduced – eg – locks, photo ids
• Cryptography is a “trust building mechanism”
• Cryptography increasingly relevant in every aspect of our life
At the crux of cryptography is the assumption that

\[
\text{TRUST} = \text{SECRET}
\]

How do we leverage a secret to build trust?
Cryptographic Primitives.
Components of Trust
  Secrecy, Authentication, Non-repudiation, Integrity, Identity
Cryptographic Primitives
  Encryption/Decryption, Digital Signatures, Hash (one-way) functions, random sequence generators
Cryptography

Encryption and Decryption

Two ways

Symmetric Cryptography (shared key)
Asymmetric Cryptography (two-key / public-key)
An Analogy - Shared Secret as a Key

Alice and Bob share a key to a lock
Handling messages
   Put them in a box
   Secure the box with the lock
Alice knows only Bob has a key (and vice-versa)
Shared key enables trust
Modern cryptography uses bits and algorithms (computer programs) instead.
Asymmetric Key Cryptography

Encrypt with **public** key
Decrypt with **private** key

Private key is secret, public key is not (could be made available in some on-line public directory)

Used for

Secrecy and Digital Signatures
Asymmetric Key Cryptography

- Alice, Bob and Oscar - have never met before (no shared secret)
- Alice announces her public key to Bob (Oscar also listens)
- Bob chooses a secret randomly and encrypts it with Alice's public key and announces the result
- Alice can decrypt Bob's message and determine Bob's chosen secret – Oscar cannot (he does not have access to Alice's Private key)
- Now Alice and Bob have a shared secret!
- Notion of Public key cryptography is definitely not intuitive!
Paper and Pencil Cryptography
First documented use by Julius Caesar
Caesar Cipher (Enciphering and Deciphering)
- MEET YOU TOMORROW (Plain Text)
  RJJY DTZ YTRTWWTB (Cipher Text)
26 possible keys – (0-25, key 5 used in example above)
Vignere Cipher (26 x m keys)
- MEET Y O U T O M O R R O W
  DOGDOGDOGDOGDOG (4,15,7), m=3
- PSKWMUHXHU P CX U C C
More P&P Ciphers

Auto-key Vignere Cipher
MEET YOU TOMORROW (Plain Text)
HIYA (key)

Extended key
HIYAMEETYOUTOMO

Cipher
MEETYOUTOMORROW
HIYAMEETYOUTOMO
TMCtalkksymmaikfaK
Even More Ciphers!

A more complex substitution Cipher
  Each letter substituted by an arbitrary letter
  Full Vignere.

Full Vignere key generation
  NETWORKSECURITY ANDCRYPTOGRAPHYBIZ
  NETWORKSCU IYA DPGHBZFJ LMQVX
  ABCD EFGHI J KLMNOPQRSTUVWXYZ
  26! (403291461126605635584000000) keys

Permutation Ciphers
  Text length M AND -> (2,3,1) -> NDA
  M! possible permutations
Substitution & Permutation

- Why only substitution and permutation?
- Both are reversible operations (so you can decrypt)
- Old ciphers used one or the other
- Modern ciphers use both
  - Repeatedly