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 – photo ids
- Cryptography is a “trust building mechanism”
- We are at a point (or about to arrive at a point) where cryptography needs to be part of our day-to-day lives
At the crux of cryptography is the assumption that

**TRUST = SHARED SECRET**

How do we leverage shared secret to build trust?

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

```
Plain Text  Encryption  Cipher Text

Cipher Text  Decryption  Plain Text
```

• 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 computer programs – not locks and keys!
Asymmetric Key Cryptography

- Encrypt with **public** key
- Decrypt with **private** key
- Private key is secret, public key is not (could be entered 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
- 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!
Illustration of Asymmetric Key Cryptography

- Simple box with a lock won't work; need a more sophisticated contraption!
- Message box (locker) with trapdoors
- Encryption and Digital Signatures
- “Front door” opened with public key to drop messages for Alice and collect documents signed by Alice
- “Back door” can be opened only by Alice with her private key.
- Only an analogy.
- Need “trapdoor one-way” functions to realize asymmetric cryptography.
Paper and Pencil Cryptography

- Read Sections 2.1 through 2.3 of text
- Evolution of 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
  - DOGD OGD OGD OGD OGD OGD OGD OGD
  - PSK W M UXHU PCX UCC
  - (4,15,7), m=3
More P&P Ciphers

- Auto-key Vignere Cipher
  - MEET YOU TOMORROW (Plain Text)
  - HIYA (key)
- Extended key
  - HIYAMEETYOUTOMO
- Cipher
  - MEETYOUTOMORROW
  - HIYAMEETYOUTOMO
  - TMCTKSYMMAIKFAK
Even More Ciphers!

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

- Key generation
  - NETWORKSECURITY ANDCRYPTOGRAPHYBIZ
  - NETWORKSCU IYA DPGHBZFJ LMQVX
  - ABCD EFGHI J KLMNOPQRSTU VWXYZ
  - 26! (403291461126605635584000000) keys

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

- Combination of substitution and permutation

- Repeated application – many rounds
Let's do some math!

- Mathematics is a language!
- Often when we “develop mathematical tools” we lose perspective...
- Not just about “numbers”
- Language – consists of statements
- A statement is an expression of TRUTH
- Numbers
  - Whole Numbers
  - Zero
  - Integers - Zero + Whole Numbers + Negative Whole Numbers
  - Rational numbers
  - Real numbers
  - Complex numbers
Modular Arithmetic
(Read Sections 4.1 thro 4.4)

- Set of all integers \( Z = \{ -\infty, ..., -3, -2, -1, 0, 1, 2, 3, ..., \infty \} \)
- Set of positive integers less than \( m \)
  \[ Z_m = \{ 0, 1, 2, 3, ..., m - 1 \} \]
- We want to perform arithmetic in \( Z_m \)
- Equivalence Classes \( a \equiv b \mod m \Rightarrow a = b + cm; a, b, c, m \in \mathbb{Z} \)
- Say \( m = 5 \)
  - EC of 0 \{ ...-15, -10, -5, 0, 5, 10, ... \}
    \[-15 \equiv -10 \equiv -5 .... \equiv 0 \equiv 5 .... \mod m \]
  - EC of 1 \{ ...-14, -9, -4, 1, 6, 11, ... \}
  - EC of 2 \{ ...-13, -8, -3, 2, 7, 12, ... \}
  - EC of 3 \{ ...-12, -7, -2, 3, 8, 13, ... \}
  - EC of 4 \{ ...-11, -6, -1, 4, 9, 14, ... \}
Addition mod m

\[ a \equiv b \mod m \Rightarrow a = b + km \]
\[ c \equiv d \mod m \Rightarrow c = d + lm \]
\[ (a + c) \equiv (c + a) \mod m \]
\[ (a + c) \equiv (b + d) \equiv (a + d) \equiv (b + c) \mod m \]
\[ (a + c) = b + d + (k + l)m = (b + d) + jm \]
Multiplication mod m

\[ a \equiv b \mod m \Rightarrow a = b + km \]
\[ c \equiv d \mod m \Rightarrow c = d + lm \]
\[ ac = (b + km)(d + lm) = bd + (bl + kd + klm)m \]
\[ ac \equiv bd \mod m \]
What about division?

- Is division possible in \( \mathbb{Z} \)?
- Group, Abelian Group, Ring and Field
  - Group
    - Addition is closed, associative
    - Existence of additive identity, additive inverse
  - Abelian group – addition is also commutative
  - Ring
    - Multiplication is closed, associative, commutative, multiplicative identity, distributive
- Field – every element except “additive identity” has multiplicative inverse
Multiplicative Inverse

- Additive identity is 0
- Multiplicative identity is 1
- Consider $m = 5$
  - $2 \to$ multiplicative inverse is 3 as $2 \times 3 \equiv 1 \mod 5$
  - $3 \to 2$
  - $4 \to 4$ \quad $4 \times 4 \equiv 1 \mod 5$
  - Obviously 1 is its own inverse
- Now $m = 6$
  - $5 \to$ inverse is 5 as \quad $5 \times 5 \equiv 1 \mod 6$
  - What about 2, 3 and 4? No inverses - why?
Basic Theorems of Arithmetic

- Let $p_i$ represent the $i^{th}$ prime

$$n = \prod_{i=1}^{\infty} p_i^{e_i}, e_i > 0$$

$$n = \prod_{i=1}^{\infty} p_i^{n_i}$$

$$m = \prod_{i=1}^{\infty} p_i^{m_i}$$

$$\text{lcm}(m, n) = \prod_{i=1}^{\infty} p_i^{\max(n_i, m_i)}$$

$$\text{gcd}(m, n) = \prod_{i=1}^{\infty} p_i^{\min(n_i, m_i)}$$
Preliminaries

- \( \text{gcd}(m,n) \) is usually represented as \((m,n)\)
- If \( n = km \), (and \( k \) is an integer) we say \( m \mid n \)
  (\( m \) divides \( n \))
- The number \( s = (m,n) \) is the largest positive integer such that \( s \mid m \) and \( s \mid n \)
- If \( (m,n)=1 \), and if \( m \mid a \) and \( n \mid a \) then \( mn \mid a \)
Algorithm for GCD

- **Basic idea** - if \(a = qb + c\) then \((a,b) = (b,c)\)
  - Let \(s = (a,b)\) and \(t = (b,c)\)
  - \(s|a, s|b, t|b, t|c\)
  - \(c = a - qb = s(a_1 - qb_1)\) or \(s|c\)
    - As \(s|b\) and \(s|c\) and \(t\) is the largest integer that divides both \(b\) and \(c\), \(s \leq t\)
  - \(a = qb + c = t(qb_2 + c_2)\) or \(t|a\)
    - As \(t|b\) and \(t|a\) and \(s\) is the largest integer that divides both \(a\) and \(b\), \(t \leq s\)
  
  \(t=s\) or \((a,b) = (b,c)\) if \(a = qb + c\)
Euclidean Algorithm

\[(a_0, a_1), a_0 > a_1\]
\[a_0 = q_1 a_1 + a_2 \Rightarrow (a_0, a_1) = (a_1, a_2)\]
\[a_1 = q_2 a_2 + a_3 \Rightarrow (a_1, a_2) = (a_2, a_3)\]
\[\vdots\]
\[a_{i-1} = q_i a_i + a_{i+1} \Rightarrow (a_{i-1}, a_i) = (a_i, a_{i+1})\]
\[\vdots\]
\[a_{r-2} = q_{r-1} a_{r-1} + a_r\]
\[a_{r-1} = q_r a_r + 0 \Rightarrow (a_{r-1}, a_r) = a_r = (a_{r-2}, a_{r-1}) = \cdots = (a_0, a_1)\]
Euclidean Algorithm

- \((457, 283)\)
Euclidean Algorithm

- $(457, 283)$
- $457 = 1 \times 283 + 174$
Euclidean Algorithm

- $(457, 283)$
- $457 = 1 \times 283 + 174$
- $283 = 1 \times 174 + 109$
- $174 = 1 \times 109 + 65$
- $109 = 1 \times 65 + 44$
- $65 = 1 \times 44 + 21$
- $44 = 2 \times 21 + 2$
- $21 = 10 \times 2 + 1$
Euclidean Algorithm

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\)
- \(283 = 1 \times 174 + 109\)
- \(174 = 1 \times 109 + 65\)
- \(109 = 1 \times 65 + 44\)
- \(65 = 1 \times 44 + 21\)
- \(44 = 2 \times 21 + 2\)
- \(21 = 10 \times 2 + 1\)
- \(2 = 2 \times 1 + 0\) \quad \text{or} \quad (457, 283) = (2, 1) = 1
Euclidean Algorithm

- $(457, 283)$
- $457 = 1 \times 283 + 174$
- $283 = 1 \times 174 + 109$
- $174 = 1 \times 109 + 65$
- $109 = 1 \times 65 + 44$
- $65 = 1 \times 44 + 21$
- $44 = 2 \times 21 + 2$
- $21 = 10 \times 2 + 1$
- $1 = 21 - 10 \times 2$
- $2 = 2 \times 1 + 0$ or $(457, 283) = (2, 1) = 1$


Euclidean Algorithm

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\)
- \(283 = 1 \times 174 + 109\)
- \(174 = 1 \times 109 + 65\)
- \(109 = 1 \times 65 + 44\)
- \(65 = 1 \times 44 + 21\)
- \(44 = 2 \times 21 + 2\)
- \(21 = 10 \times 2 + 1\)
- \(2 = 2 \times 1 + 0\)

or \((457, 283) = (2,1) = 1\)
Euclidean Algorithm (Extended)

- \((457, 283)\)
- \(457 = 1*283 + 174\) \(1 = 135*457 + (-218)*283\)
- \(283 = 1*174 + 109\)
- \(174 = 1*109 + 65\)
- \(109 = 1*65 + 44\)
- \(65 = 1*44 + 21\)
- \(44 = 2*21 + 2\) \(1 = 21-10*(44-2*21)\)
- \(21 = 10*2 + 1\) \(1 = 21-10*2\)
- \(2 = 2*1 + 0\) or \((457,283) = (2,1) = 1\)
Bezout's Representation

- $s = (a, b) = ia + jb$
- $s$ is the *smallest strictly positive integer* that can be written as a combination of $a$ and $b$
- If coins are minted in only two denominations $a$ and $b$ can we accomplish any transaction?
- How can you mark 1 foot with two scales – one 9 feet long and the other 7 feet long?
Modular Inverse

Does inverse of \( a \mod m \) exist?

\[ aa^{-1} \equiv 1 \mod m \]

Let \( b = a^{-1} \)

\[ ab \equiv 1 \mod m \Rightarrow ab = 1 + km \Rightarrow 1 = (-b)a + km \]

\( (a, m) = 1 \)

Inverse exists only if \( (a, m) = 1 \)

If \( (a, m) = 1 \) then \( a \) is “relatively prime” to \( m \)

No wonder we couldn't find inverses for 2, 3 and 4 in mod 6

Note that \( (5, 6) = 1 \) (so 5 has an inverse in mod 6)
Euclidean Algorithm (Extended)

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\) \quad \(1 = 135 \times 457 + (-218) \times 283\)
- \(283 = 1 \times 174 + 109\)
- \(174 = 1 \times 109 + 65\)
- \(109 = 1 \times 65 + 44\)
- \(65 = 1 \times 44 + 21\)
- \(44 = 2 \times 21 + 2\) \quad \(1 = 21 - 10 \times (44 - 2 \times 21)\)
- \(21 = 10 \times 2 + 1\) \quad \(1 = 21 - 10 \times 2\)
- \(2 = 2 \times 1 + 0\) \quad \text{or} \quad (457, 283) = (2, 1) = 1
Euclidean Algorithm (Extended)

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\) \(1 = 135 \times 457 + (-218) \times 283\)
- \(283 = 1 \times 174 + 109\) \((-218 \times 283) = 1 + (-135) \times 457\)
- \(174 = 1 \times 109 + 65\) \((-218 \times 283) \equiv 1 \mod 457\)
- \(109 = 1 \times 65 + 44\) \(-218 \equiv 239 \mod 457\)
- \(65 = 1 \times 44 + 21\) \((239 \times 283) \equiv 1 \mod 457\)
- \(44 = 2 \times 21 + 2\)
- \(21 = 10 \times 2 + 1\) \(1 = 21 - 10 \times 2\)
- \(2 = 2 \times 1 + 0\) \(\text{or } (457, 283) = (2, 1) = 1\)
Euclidean Algorithm (Extended)

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\) \(\Rightarrow 1 = 135 \times 457 + (-218) \times 283\)
- \(283 = 1 \times 174 + 109\) \((-218 \times 283) = 1 + (-135) \times 457\)
- \(174 = 1 \times 109 + 65\) \((-218 \times 283) \equiv 1 \mod 457\)
- \(109 = 1 \times 65 + 44\) \(-218 \equiv 239 \mod 457\)
- \(65 = 1 \times 44 + 21\) \((239 \times 283) \equiv 1 \mod 457\)
- **239 is the inverse of 283 mod 457**
- \(239 \times 283 = 67637 = 1 + 148 \times 457\)
Prime Modulus

- What if \( m \) is prime?
- We have \( \mathbb{Z}_m = \{0,1,2,...,m-1\} \)
- Every number is relatively prime to a prime number!
- So every number 1 ... m-1 has an inverse!
- \( \mathbb{Z}_m \) forms a FIELD
- Normally referred to as prime field \( \mathbb{Z}_p \)
Why prime modulus?

- It is a field
  - Almost all mathematical operations are supported.
  - Crunch away!
- Cannot decipher "patterns"
  - Deterministic mathematical functions – yet the results seem random!
  - Good for cryptography!
How about Exponentiation?

- Just repeated multiplication!
- Let's choose a large prime $p$ and a generator $g$ – both are public
- Choose some number $a$, and calculate
  - $A \equiv g^a \mod p$
  - There is a simple algorithm for exponentiation involving repeated squaring - complexity $O(\log(a))$
  - No algorithm for determining $a$ from $A!$ (complexity $O(p)$!!
  - Why is this feature useful?
Diffie-Helman Key Exchange!  
(Sneak Peak)

- Alice and Bob agree on a large prime $p$ and a generator $g$
- Alice chooses a secret $a$, and calculates
  - $A \equiv g^a \mod p$ – $A$ is Alice's public key
- Bob chooses a secret $b$, and calculates
  - $B \equiv g^b \mod p$ – $B$ is Bob's public key
- Alice and Bob exchange $A$ and $B$ in public
  - Alice calculates $S \equiv B^a \mod p \equiv g^{ba} \mod p$
  - Bob calculates $S \equiv A^b \mod p \equiv g^{ab} \mod p$
- Nobody else can calculate $S$
  - even if they know $A, B, g$ and $p$!
  - only $g^{a+b} \mod p$ (or $g^{a-b}$) – not very useful!
RECAP

- \( Z_m = \{0,1,2,...,m-1\} \)
  - \( Z_m \) is a ring – addition, multiplication...
  - Multiplicative inverse of \( a \) in \( Z_m \) exists only if
    - \( (a,m)=1; \)
    - GCD – Euclidean algo
    - Multiplicative Inverse – Extended Euclidean Algorithm
- If \( m = p \) (a prime) then \( Z_p \) is a field
  - Supports all regular operations – addition, subtraction, multiplication and multiplicative inverses
  - All elements of the field (except additive identity) has a multiplicative inverse.
Matrix Operations in a Field

\[
\begin{bmatrix}
1 & 2 & 3 \\
4 & 5 & 7 \\
8 & 6 & 4
\end{bmatrix} \mod 11
\]

\[
A^{-1} \equiv \det(A)^{-1} \adj(A) \mod 11
\]

\[
\det(A) \equiv 10 \mod 11; \inv(10) \mod 11 \equiv 10 \mod 11
\]

\[
\adj(A) \equiv \begin{bmatrix}
(20-42) & -(16-56) & (24-40) \\
-(8-18) & (4-24) & -(6-16) \\
(14-15) & -(7-12) & (5-8)
\end{bmatrix}^T \mod 11
\]

\[
\adj(A) \equiv \begin{bmatrix}
-22 & 40 & -16 \\
10 & -20 & 10 \\
-1 & 5 & -3
\end{bmatrix}^T \mod 11 \equiv \begin{bmatrix}
0 & 7 & 6 \\
10 & 2 & 10 \\
10 & 5 & 8
\end{bmatrix}^T
\]

\[
A^{-1} \equiv 10 \cdot \begin{bmatrix}
0 & 10 & 10 \\
7 & 2 & 5 \\
6 & 10 & 8
\end{bmatrix} \equiv \begin{bmatrix}
0 & 1 & 1 \\
4 & 9 & 6 \\
5 & 1 & 3
\end{bmatrix} \mod 11
\]
Matrix Operations in a Ring

\[
A \equiv \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 7 \\ 8 & 6 & 4 \end{bmatrix} \mod 26
\]

\[
A^{-1} \equiv \text{det}(A)^{-1} \text{adj}(A) \mod 26
\]

\[
\text{det}(A) \equiv 10 \mod 26
\]

\[
\text{inv}(10) \mod 26 \equiv ???
\]

\[
(10,26) \neq 1
\]

Not Invertible?

Not necessarily

No unique inverse
Hill Cipher

\[
K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 7 \end{bmatrix} \mod 26
\]

\[
\text{det}(K)^{-1} \equiv 11 \mod 26
\]

\[
K^{-1} = \begin{bmatrix} 10 & 9 & 3 \\ 7 & 17 & 22 \\ 10 & 0 & 19 \end{bmatrix} \mod 26
\]

\[
P = \begin{bmatrix} 4 \\ 3 \\ 5 \end{bmatrix} \mod 26; C = KP = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 9 \\ 23 \end{bmatrix} \mod 26
\]

\[
K^{-1}C = \begin{bmatrix} 10 & 9 & 3 \\ 7 & 17 & 22 \\ 10 & 0 & 19 \end{bmatrix} \begin{bmatrix} 14 \\ 9 \\ 23 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 3 \\ 5 \end{bmatrix}
\]
In Hill cipher the encoding key is $K$ and the decoding key is $K^{-1}$ – does this mean Hill cipher is an “asymmetric” cipher? Why?

For a 3x3 Hill cipher there are 9 “secrets.” How many known plain-text cipher-text pairs do we need to break the secret?
ATTACK ON HILL CIPHER

\[ K \equiv \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 7 \end{bmatrix} \mod 26; K^{-1} \equiv \begin{bmatrix} 10 & 9 & 3 \\ 7 & 17 & 22 \\ 10 & 0 & 19 \end{bmatrix} \mod 26 \]

\[ P_1 \equiv \begin{bmatrix} 4 \\ 3 \\ 5 \end{bmatrix} \mod 26; P_2 \equiv \begin{bmatrix} 4 \\ 21 \\ 18 \end{bmatrix} \mod 26; P_2 \equiv \begin{bmatrix} 7 \\ 16 \\ 8 \end{bmatrix} \mod 26 \]

\[ C_1 \equiv KP_1 \equiv \begin{bmatrix} 14 \\ 9 \\ 23 \end{bmatrix} \mod 26; C_2 \equiv \begin{bmatrix} 21 \\ 8 \\ 20 \end{bmatrix} \mod 26; C_3 \equiv \begin{bmatrix} 15 \\ 5 \\ 24 \end{bmatrix} \mod 26; \]

\[ \begin{bmatrix} 14 & 21 & 15 \\ 9 & 8 & 5 \\ 23 & 20 & 24 \end{bmatrix} \equiv K \begin{bmatrix} 4 & 4 & 7 \\ 3 & 21 & 16 \\ 5 & 18 & 8 \end{bmatrix} \text{ or } P \equiv KC \mod 26 \]

\[ K \equiv PC^{-1} \mod 26 \]
Find $K$ in mod 79.
Brute-force Attacks on Ciphers

- $C = E(P,K)$. We have $P$
- Try every possible key $K$
- $P_i = D(C,K_i)$
- How do we know when to stop? Under any key there will be a corresponding $P_i$
- How do we know that a particular $P_i$ is the correct plaintext?
- Does this mean brute force attacks are not possible?
Entropy of Plain Text

- Think of all possible 100 character strings that “make sense”
- For example, say a billion books, each with 1 billion “strings that make sense” - still makes it only $10^{18}$ possible phrases!
- How many total strings of length 100?
  - $26^{100}$. That is more than $3 \times 10^{141}$!
- Say we encrypt a meaningful string with a 64 bit key,
  - the ciphertext is decrypted with another key
  - What is the probability that the wrong key results in a string that makes sense?
    - $2^{64} \times 10^{18}/(3 \times 10^{141}) < 6 \times 10^{-105}$
    - Which is good news for the attacker...
Vernam Cipher
The Ultimate Cipher?

• What if we make the number of possible keys the same as the number of possible plain text messages?

• One-time pad – Vernam Cipher

• Cannot try out keys any more! There is always a key which maps cipher text to every possible plain text

• No way an attacker can eliminate any message – all messages are equally likely
  - The attacker learns NOTHING!
  - Perfect Secrecy