Chapter 7: Network security

Foundations:
- what is security?
- cryptography
- authentication
- message integrity
- key distribution and certification

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice want to communicate “securely”
- Trudy, the “intruder” may intercept, delete, add messages

What is network security?

Secrecy: only sender, intended receiver should “understand” msg contents
- sender encrypts msg
- receiver decrypts msg

Authentication: sender, receiver want to confirm identity of each other

Message Integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Internet security threats

Packet sniffing:
- broadcast media
- promiscuous NIC reads all packets passing by
- can read all unencrypted data (e.g. passwords)
- e.g.: C sniffs B’s packets
**Internet security threats**

**IP Spoofing:**
- Can generate "raw" IP packets directly from application, putting any value into IP source address field
- Receiver can't tell if source is spoofed
- E.g.: C pretends to be B

![IP Spoofing Diagram](image1)

**Denial of service (DOS):**
- Flood of maliciously generated packets "swamp" receiver
- Distributed DOS (DDOS): multiple coordinated sources swamp receiver
- E.g., C and remote host SYN-attack A

![DDOS Diagram](image2)

---

**The language of cryptography**

**Symmetric key cryptography**

Substitution cipher: substituting one thing for another
- Monoalphabetic cipher: substitute one letter for another

Plaintext: `bob. i love you. alice`
Ciphertext: `nkn. s gktc wky. mgsbc`

**Example:**
- Plaintext: `bob. i love you. alice`
- Ciphertext: `nkn. s gktc wky. mgsbc`

Q: How hard to break this simple cipher?
- Brute force (how hard?)
- Other?

Public-key crypto: encrypt key `public`, decrypt key `secret`
Symmetric key crypto: DES

DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64 bit plaintext input
- How secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase ("Strong cryptography makes the world a safer place") decrypted (brute force) in 4 months
  - no known "backdoor" decryption approach
- making DES more secure
  - use three keys sequentially (3-DES) on each datum
  - use cipher-block chaining

Public Key Cryptography

**Symmetric key crypto**
- requires sender, receiver know shared secret key
- Q: how to agree on key in first place (particularly if never "met")?

**Public key cryptography**
- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver do not share secret key
- encryption key public (known to all)
- decryption key private (known only to receiver)
Public key encryption algorithms

Two inter-related requirements:

1. need $d_B(\cdot)$ and $e_B(\cdot)$ such that $d_B(e_B(m)) = m$

2. need public and private keys for $d_B(\cdot)$ and $e_B(\cdot)$

RSA: Rivest, Shamir, Adelson algorithm

RSA: Choosing keys

1. Choose two large prime numbers $p, q$ (e.g., 1024 bits each)

2. Compute $n = pq$, $z = (p-1)(q-1)$

3. Choose $e$ (with $e<\eta$) that has no common factors with $z$. ($e, z$ are “relatively prime”).

4. Choose $d$ such that $ed-1$ is exactly divisible by $z$. (in other words: $ed \mod z = 1$).

5. Public key is $(n,e)$. Private key is $(n,d)$.

RSA: Encryption, decryption

0. Given $(n,e)$ and $(n,d)$ as computed above

1. To encrypt bit pattern, $m$, compute $c = m^e \mod n$ (i.e., remainder when $m^e$ is divided by $n$)

2. To decrypt received bit pattern, $c$, compute $m = c^d \mod n$ (i.e., remainder when $c^d$ is divided by $n$)

Magic happens! $m = (m^e \mod n)^d \mod n$

RSA example:


$e=5$ (so $e, z$ relatively prime).

$d=29$ (so $ed-1$ exactly divisible by $z$).

<table>
<thead>
<tr>
<th>letter</th>
<th>$m$</th>
<th>$m^e$</th>
<th>$c = m^e \mod n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>l</td>
<td>12</td>
<td>1524832</td>
<td>17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$c$</th>
<th>$c^d$</th>
<th>$m = c^d \mod n$</th>
<th>letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>48196857210675091509141825223872000</td>
<td>12</td>
<td>l</td>
</tr>
</tbody>
</table>
RSA: Why: \[ m = (m^e \mod n)^d \mod n \]

Number theory result: If \( p, q \) prime, \( n = pq \), then
\[ x^y \mod n = x \mod n = x^y \mod (p-1)(q-1) \mod n \]

\[(m^e \mod n)^d \mod n = m^{ed} \mod n \]
\[= m^{ed} \mod (p-1)(q-1) \mod n \]
(\text{using number theory result above})
\[= m^1 \mod n \]
(\text{since we chose } ed \text{ to be divisible by } (p-1)(q-1) \text{ with remainder 1 })
\[= m \]