Security I: 8.1 to 8.3

Smith College, CSC 249
November 17, 2014

Network Security

- The principles of network security:
  - Cryptography, beyond “confidentiality”
  - Access & availability
  - Message integrity
  - Authentication
  - Securing each layer

What is network security?

Access and Availability:

Confidentiality:

Data Integrity:

Authentication:

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob and Alice want to communicate “securely”
- Trudy (intruder) may intercept, delete, add and/or alter messages
- Who/what might Alice and Bob be?
The language of cryptography

Symmetric Key Cryptography

- Both parties have the same key
- Use this key to both encrypt and decrypt the message
  → The actions are symmetric

Early - Caesar Cypher

Now, two dominant algorithms

- DES – data encryption standard
- AES – advanced encryption standard

Symmetric Key Cryptography

- Symmetric key cryptography: sender & receiver keys are identical and secret (but known by 2 parties)
- Public-key cryptography: the encryption key is public, the decryption key secret, and known only by one party

Symmetric key cryptography: DES

- DES operation
  - Initial permutation
  - 16 identical "rounds" of function application, each using different 48 bits of key
  - Final permutation

AES: Advanced Encryption Standard

- Symmetric-key NIST standard
  - Replaced DES (Nov 2001)
- Processes data in 128 bit blocks
  - 128, 192, or 256 bit keys
- Brute force decryption (try each key)
  - Taking 1 sec on DES, takes 149 trillion years for AES
**Symmetric key cryptography**

- Bob and Alice share/know the same (symmetric) key: \( K \)
  - e.g., key is knowing substitution pattern in mono-alphabetic substitution cipher
- **Q:** how do Bob and Alice agree on key value?

**Public key cryptography**

- **Q:** how do Bob and Alice agree on key value?

**RSA Important Property**

- The following property defines this method:
  \[ K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m)) \]
  - use public key first, followed by private key
  - use private key first, followed by public key
Public key encryption algorithms

Requirements:

1. need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that $K_B^-(K_B^+(m)) = m$

2. given public key $K_B^+$, it should be impossible to compute private key $K_B^-$

RSA: Rivest, Shamir, Adelson algorithm

RSA: Choosing keys (an art)

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 $e \cdot n$) 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 Example:


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

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

encrypt:          letter m  m\text{e}  c = m\text{e} \mod n

<table>
<thead>
<tr>
<th></th>
<th>letter</th>
<th>m</th>
<th>m\text{e}</th>
<th>c = m\text{e} \mod n</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>l</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

decrypt:         c  c\text{d} m = c\text{d} \mod n  letter

<table>
<thead>
<tr>
<th></th>
<th>letter</th>
<th>c\text{d}</th>
<th>m = c\text{d} \mod n</th>
<th>letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>l</td>
<td>12 \text{d}</td>
<td>12 \text{d} \mod 35</td>
<td>l</td>
</tr>
</tbody>
</table>
Using RSA, choose $p = 3$, $q = 11$. Encode a letter of your choice and send it to a different host to decode.

**Suggestion for $e$?** ... choose $e = 9$.

Then $z = (p-1)(q-1) =$

Also choose $d =

  - so $e \cdot d$
  - $e \cdot d - 1 =$

Thus $n =$

---

**Public Key Cryptography Concerns?**

- It must be very difficult to discover or determine private keys
- Since encryption keys are public, entities can claim to be someone else when sending a message
  - Need more than just public key cryptography
  - ... Need to bind the message to a sender

---

**Next Security Tasks**

- Encryption keys are public, so anyone could claim to be someone else
  - Need more than public key cryptography
- ... Need to bind the message to a sender

- Message integrity & end-point authentication
  1) Cryptographic hash function
  2) Digital signature