Network Security Contd

COMP90007

Internet Technologies

Public Key Algorithms

- Fundamentally different to symmetric key ones
- Diffe & Hellman proposed the new model
  - **Asymmetric keys**
  - **Key used to encrypt and key used to decrypt different**
  - Not easily derivable from each other
  - Hence addressing a fundamental issue of key sharing
- Diffe-Hellman key system
  - **Key 1: public key**, usable by anyone **to encrypt** messages to the owner of the key, this key known to all
  - **Key 2: private key**, required **to decrypt** the message and known only by the owner of this key

The Process

- C = ciphertext, P = plaintext, E = encryption, D=decryption
  K1, K2 = keys

- $C = E_{K1}(P)$
  - Sender knows the public key K1 and the P

- $P = D_{K2}(C)$
  - Only receiver knows private K2 which can undo K1’s effect

- $D_{K2}(E_{K1}(P)) = P$

RSA: An Asymmetric Key Algorithm

- **<u>RSA - Rivest, Shamir, Adleman</u>**
- Famous and robust algorithm
- Key generation:
  - Choose two large primes, p and q
  - Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
  - Choose d to be relatively prime to z, i.e., no common factors
  - Find e such that
    - **$(d \times e) \bmod z = 1$**
  - Public key is (e, n), and private key is (d, n)
- Encryption:
  - $Cipher = Plain^{e} \pmod{n}$
- Decryption:
  - $Plain = Cipher^{d} \pmod{n}$

RSA Security

- RSA's security is **based on the difficulty involved in factoring large numbers in math theory** - approx 10^{25} years to factor a 500 digit number and RSA uses 1024 bits!
- RSA is too slow for encrypting/decrypting large volumes of data, but is widely used for many other things such as **secure key distribution**
- RSA can be used in tandem with symmetric key algorithms

RSA Example

- Let p=3, q=11: then ***z*** is (3 – 1) x (11 – 1) = 20
- What is a potential d?
- If d = 7 then z and 20 has no common factors
- What is an e?
- If e = 3, then (d x e) is 1 in mod z
- What are the two key tuples then?
- Enc: 3. 33 Dec: 7. 33 (as n=3 x 11=33 and d=7 and e=3)

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Encryption: $C = P^3 \bmod 33$

Decryption: $P = C^7 \bmod 33$

S is the 19th character in the alphabet…

Another Use of Cryptography: Digital Signatures

- Cryptographic approaches can also be used to ensure authenticity and allow for non-repudiation
- Requirements
  - Receiver can ***verify the claimed identity of the sender***
  - ***Sender cannot deny she created*** contents of the message
  - ***Receiver cannot have derived the message themselves***
- Three approaches
  - Using symmetric keys via an intermediary
    - You need a BIG BROTHER to do all the messaging, not good!
  - Using **public keys** as individuals

Using Public Keys

- Sender Alice uses ***private key on P***
- ***Receiver Bob uses her public key to undo and get P***
- RSA can do this as well, as ***E(D(P)) = P in RSA***

- Alice cannot deny signing as she only knows her private key

Signatures with Message Digests

- Basic concept of a **message digest is to use a one-way hash function** for an arbitrary length of plaintext, so that it becomes a ***"unique" small fixed-length bit string***

- Thus **no need to deal with huge message text and encryption just for authentication** purposes

- A message digest (MD) has four important properties:
  - 1 Given P, it is easy to compute MD(P)
  - 2 Given MD(P) it is effectively impossible to find P
  - 3 Given P, no one can find P' such that MD(P') = MD(P)
  - 4 A change in even a single bit of input produces a very different output

Famous Message Digest Algorithms

- MD5
- SHA-1
- Outputs
  - Given ”this is a test“ (text could have been longer)
  - MD5:

    e19c1283c925b3206685522acfe3e6
  - SHA-1:

    6476df3aac780622368173fe6e768a2edc3932c8

Public Key Management

- There is **specific PK infrastructure** to avoid compromising the security of PK's **during the initial distribution process**.
- Certification Authority (CA)
  - A trusted intermediary who uses non-electronic identification to identify users prior to certifying keys and certificates
- X.509
  - An international standard for certificate expression
- PKI (Public Key Infrastructure) is a
  - **Hierarchically structured certificate authorities** allow for the establishment of a chain of trust or certification path
  - *Verisign* was such a company

Certificate Issuing

- A Certificate authority (CA) says:

I hereby certify that the public key 19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A belongs to Robert John Smith 12345 University Avenue Berkeley, CA 94702 Birthday: July 4, 1958 Email: bob@superdupernet.com
SHA-1 hash of the above certificate signed with the CA's private key