

Principles of Information Security

CS 5323 Lecture 12

Prof. William Winsborough
October 30, 2008

Business

- Reschedule: Preliminary project proposals due Thursday, November 6 (1-2 pages)
 - Projects are of your own design
 - They can be programming or paper based
 - You can write a critique of one to three papers from the literature
 - You can present a paper in class
 - Working in teams is ok
- Questions from previous lectures?
- Portions of today's notes come from Wikipedia

30 October 2008

Winsborough CS 5323 Lecture 12

2

Why does RSA Work?

- Recall Algorithm
 - Choose two large prime numbers p, q
 - Let $n = pq$; then $\phi(n) = (p-1)(q-1)$
 - Choose $e < n$ such that e is relatively prime to $\phi(n)$.
 - Compute d such that $ed \bmod \phi(n) = 1$
 - Public key: (e, n) ; private key: d
 - Encipher: $c = m^e \bmod n$
 - Decipher: $m = c^d \bmod n$
- So why is $m^{ed} \equiv c^d \equiv m \pmod{n}$?

30 October 2008

Winsborough CS 5323 Lecture 12

3

Background: Fermat's Little Theorem

- For every prime number p and every (positive) integer a ,
 $a^p \equiv a \pmod{p}$
- It is sufficient to prove
 $a^{p-1} \equiv 1 \pmod{p}$
- Simple proof is based on "bracelets"
 - Strings of length p over an alphabet of size a
 - a^p such strings
 - Will show: if we remove all strings consisting of just a single symbol, the rest can be collected into groups of size p

30 October 2008

Winsborough CS 5323 Lecture 12

4

Bracelets

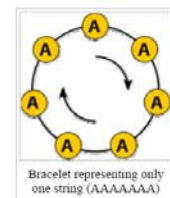
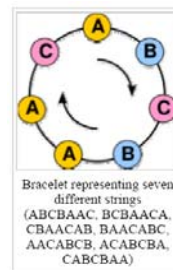
- Given any string, consider the set of strings called *friends* that can be obtained from it by rotation
- Suppose a string S can be broken down in to repeated copies of a string T , but T cannot be further broken down
 - Then the length of T is the number of friends S has
- If the length of S is a prime, it cannot be broken down further

30 October 2008

Winsborough CS 5323 Lecture 12

5

Bracelets



30 October 2008

Winsborough CS 5323 Lecture 12

6

Completing the Proof

- There are a strings consisting of just one of the a symbols
- The other $a^p - a$ strings each have $p - 1$ friends (because p is prime)
 - These can be grouped into sets of friends, each set having size p
 - So $a^p - a$ is divisible by p

30 October 2008

Winsborough CS 5323 Lecture 12

7

Stolen from Wikipedia

Now, $ed \equiv 1 \pmod{(p-1)(q-1)}$, and hence

$$\begin{aligned} ed &\equiv 1 \pmod{p-1} \text{ and} \\ ed &\equiv 1 \pmod{q-1} \end{aligned}$$

which can also be written as

$$\begin{aligned} ed &= k(p-1) + 1 \text{ and} \\ ed &= h(q-1) + 1 \end{aligned}$$

for proper values of k and h . If m is not a multiple of P then m and P are coprime because P is prime; so by Fermat's little theorem

$$m^{(p-1)} \equiv 1 \pmod{p}$$

and therefore, using the first expression for ed ,

30 October 2008

Winsborough CS 5323 Lecture 12

8

Stolen, Cont.

$$m^{ed} = m^{k(p-1)+1} = (m^{p-1})^k m \equiv 1^k m = m \pmod{p}$$

If instead m is a multiple of P , then

$$m^{ed} \equiv 0^{ed} = 0 \equiv m \pmod{p}$$

Using the second expression for ed , we similarly conclude that

$$m^{ed} \equiv m \pmod{q}$$

Since P and q are distinct prime numbers, they are relatively prime to each other, so the fact that both primes divide $m^{ed} - m$ implies their product Pq divides $m^{ed} - m$, which means

$$m^{ed} \equiv m \pmod{pq}$$

Thus,

$$c^d \equiv m \pmod{n}$$

30 October 2008

Winsborough CS 5323 Lecture 12

9

Cryptographic Checksums

- Mathematical function to generate a set of k bits from a set of n bits (where $k \leq n$).
 - k is smaller than n except in unusual circumstances
- Example: ASCII parity bit
 - ASCII has 7 bits; 8th bit is “parity”
 - Even parity: even number of 1 bits
 - Odd parity: odd number of 1 bits

30 October 2008

Winsborough CS 5323 Lecture 12

10

Example Use

- Bob receives “10111101” as bits.
 - Sender is using even parity; 6 1 bits, so character was received correctly
 - Note: could be garbled, but 2 bits would need to have been changed to preserve parity
 - Sender is using odd parity; even number of 1 bits, so character was not received correctly

30 October 2008

Winsborough CS 5323 Lecture 12

11

Definition

- Cryptographic checksum $h: A \rightarrow B$:
 1. For any $x \in A$, $h(x)$ is easy to compute
 2. For any $y \in B$, it is computationally infeasible to find $x \in A$ such that $h(x) = y$
 3. It is computationally infeasible to find two inputs $x, x' \in A$ such that $x \neq x'$ and $h(x) = h(x')$
 - Alternate form: Given any $x \in A$, it is computationally infeasible to find a different $x' \in A$ such that $h(x) = h(x')$.

30 October 2008

Winsborough CS 5323 Lecture 12

12

Collisions

- If $x \neq x'$ and $h(x) = h(x')$, x and x' are a *collision*
 - Pigeonhole principle: if there are n containers for $n+1$ objects, then at least one container will have 2 objects in it.
 - Application: if there are 32 files and 8 possible cryptographic checksum values, at least one value corresponds to at least 4 files

30 October 2008

Winsborough CS 5323 Lecture 12

13

Keys

- Keyed cryptographic checksum: requires cryptographic key
 - DES in chaining mode: encipher message, use last n bits. Requires a key to encipher, so it is a keyed cryptographic checksum.
- Keyless cryptographic checksum: requires no cryptographic key
 - MD5 and SHA-1 are best known; others include MD4, HAVAL, and Snefru

30 October 2008

Winsborough CS 5323 Lecture 12

14

HMAC

- Generic term for using a keyless cryptographic checksum function and a cryptographic key to make keyed cryptographic checksum
 - Let h be keyless cryptographic checksum function that takes data in blocks of b bytes and outputs blocks of l bytes.
 - Let k' be a cryptographic key of length b bytes
 - If short, pad with 0 bytes; if long, hash to length b
- $\text{HMAC-}h(k, m) = h(k' \oplus \text{opad} || h(k' \oplus \text{ipad} || m))$
 - \oplus exclusive or, $||$ concatenation
 - ipad is 00110110 repeated b times
 - opad is 01011100 repeated b times

30 October 2008

Winsborough CS 5323 Lecture 12

15

Key Points

- Two main types of cryptosystems: classical and public key
- Classical cryptosystems encipher and decipher using the same key
 - Or one key is easily derived from the other
- Public key cryptosystems encipher and decipher using different keys
 - Computationally infeasible to derive one from the other
- Cryptographic checksums provide a check on integrity

30 October 2008

Winsborough CS 5323 Lecture 12

16