

ICS 134

Homework 2 Solution

Due Friday January 26, 5pm PST
Submission by email to the TA: plaintext or PDF only.

1. SOLUTION

The good guys will take advantage of the advance in computer speed:

n = length of the key

$t(n)$ = time to encrypt = $c \cdot n$, where c is a constant.

$T(n)$ = time to brute force = $2^{n-1} t(n)$

$t'(n)$ = time to encrypt with faster computer = $t(n)/2$

$T'(n)$ = time to brute force with faster computer = $T(n)/2$

Without decreasing performances, keys can be now of length $2 \cdot n$. The time to brute force will be:

$$T'(2 \cdot n) = T(2 \cdot n)/2 = \frac{2^{2n-1}}{2} 2cn = 2^n T(n)$$

2. SOLUTION

A:

By contradiction, suppose there are two DIFFERENT identity elements I and J.

Because the group is abelian, it has the property of commutativity

$$I @ X = X @ I = X$$

Then

$$I @ J = J @ I = I$$

and

$$J @ I = I @ J = J$$

It's absurd that the same operation on the same operands output two different elements. This means that our assumption was wrong and that $I = J$.

B:

By contradiction, suppose Y and Z represent two DIFFERENT inverses of X.

$$\begin{aligned} Y @ X @ Z &= (Y @ X) @ Z && \text{(by associativity)} \\ &= I @ Z && \text{(by the inverse property)} \\ &= Z && \text{(by the identity property)} \end{aligned}$$

also

$$\begin{aligned} Y @ X @ Z &= Y @ (X @ Z) && \text{(by associativity)} \\ &= Y @ I && \text{(by the inverse property)} \\ &= Y && \text{(by the identity property)} \end{aligned}$$

As in part A, the operation on the same operands outputs two different elements...

3. SOLUTION:

A:

Number the steps of the Euclidean algorithm starting with step 0. The quotient obtained at step i is denoted by q_i . As we carry out each step of the Euclidean algorithm, we also calculate an auxiliary number, p_i . For the first two steps, the value of this number is given: $p_0 = 0$ and $p_1 = 1$. For the remainder of the steps, we recursively calculate $p_i = p_{i-2} - p_{i-1} * q_{i-2} \pmod{n}$. Continue this calculation for one step beyond the last step of the Euclidean algorithm.

If the last non-zero remainder occurs at step k , then if this remainder is 1, x has an inverse and it is p_{k+2} .

0) $209 = 113 + 96$	$p_0 = 0$
1) $113 = 96 + 17$	$p_1 = 1$
2) $96 = 17 * 5 + 11$	$p_2 = 0 - 1 \pmod{209} = 208$
3) $17 = 11 + 6$	$p_3 = 1 - 208 \pmod{209} = 2$
4) $11 = 6 + 5$	$p_4 = 208 - 10 \pmod{209} = 198$
5) $6 = 5 + 1$	$p_5 = 2 - 198 \pmod{209} = 13$
6) $5 = 5 + 0$	$p_6 = 198 - 13 \pmod{209} = 185$
	$p_7 = 13 - 185 \pmod{209} = 37$

Check: $113 * 37 = 4181 = 1 \pmod{209}$

B:

$209 = 11 * 19$, so $\phi(209) = (11 - 1) * (19 - 1) = 180$

C:

Factors of 208 = 2, 13.

$\phi(208) = 208 * (1 - 1/2) * (1 - 1/13) = 96$

4. SOLUTION:

A:

There exist 10^{12} possible id numbers. We therefore need $1.17 \cdot \text{SQRT}(10^{12}) = 1.17 \cdot (10^6) = \text{approx } 1,170,000$ students in order to have a 50% of a collision occurring.

B:

Chances of choosing the inverted id are the equals the chances of choosing the same id.

5. The plaintext of the corrupted block cannot be retrieved, but any other block is not affected by the error.
6. Because blocks might arrive damaged, a hash is required to provide integrity. Because blocks might arrive in a random order, also a sequential number is needed (this will allow Bob to reorder packets and to detect missing ones).

