Some Solutions to HW05 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

HW05, Problem 2a

Alice and Bob are doing Diffie Hellman with $p = 31$ and $g = 2$. Note that g is NOT a generator. Alice uses $a = 8$ and Bob uses $b = 9$. What is the shared secret key? Express as a number in $\{0, \ldots, 30\}$

HW05, Problem 2a

Alice and Bob are doing Diffie Hellman with $p = 31$ and $g = 2$. Note that g is NOT a generator. Alice uses $a = 8$ and Bob uses $b = 9$. What is the shared secret key? Express as a number in $\{0, \ldots, 30\}$

SOLUTION

$$(2^8)^9 \equiv 2^{72} \pmod{31} \equiv 2^{72 \pmod{30}} \pmod{31} \equiv 2^{12} \pmod{31}$$

We will now use that $2^5 = 32 \equiv 1 \pmod{31}$.

$$2^{12} = 2^5 \times 2^5 \times 2^2 \pmod{31} \equiv 1 \times 1 \times 4 \pmod{31} \equiv 4 \pmod{31}.$$

HW05, Problem 2b

Why is using a non-gen bad? Use $p = 31$ and $g = 2$ to make point.

HW05, Problem 2b

Why is using a non-gen bad? Use $p = 31$ and $g = 2$ to make point.
SOLUTION
Lets look at the case at hand: $p = 31$ and $g = 2$. Math is mod 31.
The only numbs we use:

HW05, Problem 2b

Why is using a non-gen bad? Use $p = 31$ and $g = 2$ to make point.

SOLUTION

Lets look at the case at hand: $p = 31$ and $g = 2$. Math is mod 31.
The only numbs we use: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$.

HW05, Problem 2b

Why is using a non-gen bad? Use $p = 31$ and $g = 2$ to make point.

SOLUTION

Lets look at the case at hand: $p = 31$ and $g = 2$. Math is mod 31.
The only numbs we use: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$.
A & B are *not* operating in $\mathbb{Z}_{31}^*$ which has 30 elements, but in $\mathbb{Z}_5^*$ which has only 5 elements.

HW05, Problem 2b

Why is using a non-gen bad? Use $p = 31$ and $g = 2$ to make point.

SOLUTION

Lets look at the case at hand: $p = 31$ and $g = 2$. Math is mod 31.
The only numbs we use: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$.
A & B are *not* operating in $\mathbb{Z}_{31}^*$ which has 30 elements, but in $\mathbb{Z}_5^*$ which has only 5 elements.
When we pick p we want to be using $\mathbb{Z}_p^*$, not some smaller domain. If g is not a generator we will end up on $\mathbb{Z}_q^*$ where q divides $p - 1$ and hence is much smaller than p.

HW05, Problem 2b

Why is using a non-gen bad? Use $p = 31$ and $g = 2$ to make point.
SOLUTION
Lets look at the case at hand: $p = 31$ and $g = 2$. Math is mod 31.
The only numbs we use: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$.
A & B are *not* operating in $\mathbb{Z}_{31}^*$ which has 30 elements, but in $\mathbb{Z}_5^*$ which has only 5 elements.
When we pick p we want to be using $\mathbb{Z}_p^*$, not some smaller domain. If g is not a generator we will end up on $\mathbb{Z}_q^*$ where q divides $p - 1$ and hence is much smaller than p.
1) Badly written answers that referred to security got Full credit.
In future will demand clean answer.

HW05, Problem 2b

Why is using a non-gen bad? Use $p = 31$ and $g = 2$ to make point.
SOLUTION
Lets look at the case at hand: $p = 31$ and $g = 2$. Math is mod 31.
The only numbs we use: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$.
A & B are *not* operating in $\mathbb{Z}_{31}^*$ which has 30 elements, but in $\mathbb{Z}_5^*$ which has only 5 elements.
When we pick p we want to be using $\mathbb{Z}_p^*$, not some smaller domain. If g is not a generator we will end up on $\mathbb{Z}_q^*$ where q divides $p - 1$ and hence is much smaller than p.
1) Badly written answers that referred to security got Full credit. In future will demand clean answer.
2) Some students said if g is not a generator then there could be an (a, b) an (a', b') they yield THE SAME secret Key, bad for DECRYPTION. BUT DH IS NOT A CRYPTO SYSTEM. Full Credit since raised a good point. In future will demand clean correct answer.

HW05, Problem 3a

$p = 47$ and $g = 5$. Alice uses $a = 10$ and Bob uses $b = 11$. What is the shared secret key? Express as a number in $\{0, \ldots, 46\}$

HW05, Problem 3a

$p = 47$ and $g = 5$. Alice uses $a = 10$ and Bob uses $b = 11$. What is the shared secret key? Express as a number in $\{0, \dots, 46\}$

SOLUTION

$(5^{10})^{11} = 5^{110} \equiv 5^{110 \pmod{46}} \equiv 5^{18} \pmod{47} \equiv 2$

END OF SOLUTION

HW05, Problem 3b

$p = 47$ and $g = 5$. Alice uses $a = 11$ and Bob uses $b = 10$. What is the shared secret key? Express as a number in $\{0, \ldots, 46\}$.

HW05, Problem 3b

$p = 47$ and $g = 5$. Alice uses $a = 11$ and Bob uses $b = 10$. What is the shared secret key? Express as a number in $\{0, \ldots, 46\}$.

SOLUTION

$(5^{11})^{10} = 5^{110} \equiv 5^{110 \pmod{46}} \equiv 5^{18} \pmod{47} \equiv 2$

END OF SOLUTION

HW05, Problem 3c

Prove that:
Let p be a prime and g be a generator. Let $a, b \in \{0, \ldots, p-1\}$. Let $s_{a,b}$ be the shared secret key if Alice uses a and Bob uses b. Show that $s_{a,b} = s_{b,a}$.

HW05, Problem 3c

Prove that:
Let p be a prime and g be a generator. Let $a, b \in \{0, \ldots, p-1\}$.
Let $s_{a,b}$ be the shared secret key if Alice uses a and Bob uses b.
Show that $s_{a,b} = s_{b,a}$.

SOLUTION

If Alice uses a and Bob uses b then the shared secret string is g^{ab}.
If Alice uses b and Bob uses a then the shared secret string is g^{ba}.
These two are equal since $ab = ba$. This is NOT a trivial remark since one CAN do DH in domains which are not commutative.

HW05, Problem 3c

Prove that:
Let p be a prime and g be a generator. Let $a, b \in \{0, \ldots, p-1\}$. Let $s_{a,b}$ be the shared secret key if Alice uses a and Bob uses b. Show that $s_{a,b} = s_{b,a}$.

SOLUTION

If Alice uses a and Bob uses b then the shared secret string is g^{ab}.
If Alice uses b and Bob uses a then the shared secret string is g^{ba}.
These two are equal since $ab = ba$. This is NOT a trivial remark since one CAN do DH in domains which are not commutative.

Some Students on piazza asked how rigorous the proof had to be. This is **not** the kind of proof for which this question makes sense. Above is rigorous. No subtle issues.

HW05, Problem 4a

Alice and Bob are going to use RSA with primes $p = 7$ and $q = 11$. List all possible values of $e \geq 10$ that Alice could pick.

SOLUTION

$R = \phi(7) \times \phi(11) = 6 \times 10 = 60.$

e has to be rel prime to 60.

Here are all such numbers:

$$\{11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}$$

END OF SOLUTION

HW05, Problem 4b

Alice and Bob are going to use RSA with primes $p = 7$ and $q = 11$. Let e be a number NOT on the list in the last item. What goes wrong if Alice tries to use e?

SOLUTION

Since e is NOT rel prime to 60, there is no d with
$ed \equiv 1 \pmod{60}$.
So in the very next step of trying to pick d, Alice will fail.

END OF SOLUTION

HW05 Problem 5a

Alice and Bob are again using RSA with $p = 7$ and $q = 11$. Let $e = 13$ (This is a value that can be used).
What is d?

HW05 Problem 5a

Alice and Bob are again using RSA with $p = 7$ and $q = 11$. Let $e = 13$ (This is a value that can be used).
What is d?

SOLUTION

d is the inverse of 13 mod 60 so thats 37.

END OF SOLUTION

HW05 Problem 5b

Alice and Bob are again using RSA with $p = 7$ and $q = 11$ and $e = 13$. What does Alice broadcast? What does she keep secret?

SOLUTION

She broadcasts $(77, 13)$. She keeps secret 37.

END OF SOLUTION

HW05 Problem 5c

Bob wants to send 30. What does he send?

SOLUTION

Bob sends $30^{13} \pmod{77} = 72$.

END OF SOLUTION

HW05 Problem 5d

Bob sends 71. Show how Alice determines m and also give us m.

HW05 Problem 5d

Bob sends 71. Show how Alice determines m and also give us m.
SOLUTION

$$m^{13} \equiv 71 \pmod{77}$$

Raise both sides to the power 37 (the value of d).

$$m^{13\times 37} \equiv 71^{37} \equiv 36 \pmod{77}$$

KEY is that the exponents are mod 60 which is $\phi(77)$ and
$13 \times 37 \equiv 1 \pmod{60}$ so we get
$m = 36$.
END OF SOLUTION