Problem Set 5

1. Answer the following questions regarding $\mathbf{Z}_{23}^*$.
   (a) What are the elements of $\mathbf{Z}_{23}^*$? List all of them.
   (b) What is the order of this group?
   (c) What is the order of 2?
   (d) What is the order of 5?
   (e) Is $\mathbf{Z}_{23}^*$ cyclic? If your answer is "yes," provide a generator. If your answer is "no," explain your answer.

2. Prove that the hardness of the DDH problem implies the hardness of the CDH problem. Use the definitions of these problems as specified in the lecture slides.

3. Let p be an odd prime, and let G be $\mathbf{Z}_p^*$. Suppose g is a generator of $\mathbf{Z}_p^*$ but oddly enough is kept secret. Let $x \in \mathbf{Z}_{p-1}$, and let $y = g^x \bmod p$. Given inputs p, x, and y, is it possible to compute g in polynomial time in the size of the inputs? Prove your answer. You may refer to algorithms we studied in class by name without explicitly defining how they work.

4. Compute $19^{571500000} \bmod 77$ by hand. Show your work and justify all the steps in your computation.

5. Prove that DDH is easy in $\mathbf{Z}_p^*$ when p is an odd prime. Here, you may use without proof, the properties we studied in class about the Legendre (equivalently in this context, the Jacobi) symbol.

6. Suppose DDH is hard for a group G. Consider the ElGamal encryption scheme $(\mathsf{KG}, \mathcal{E}, \mathcal{D})$ based on G as studied in class and recalled here for your convenience. (In the description, g is a generator of G, and m is its order.) Is this scheme secure under IND-CCA? Prove your answer.

Alg KG	**Alg** $\mathcal{E}_X(M)$	**Alg** $\mathcal{D}_x(Y, W)$
$x \xleftarrow{\$} \mathbf{Z}_m$	$y \xleftarrow{\$} \mathbf{Z}_m$; $Y \leftarrow g^y$	$K \leftarrow Y^x$
$X \leftarrow g^x$	$K \leftarrow X^y$	$M \leftarrow W \cdot K^{-1}$
Return (X, x)	$W \leftarrow K \cdot M$	Return M
	Return (Y, W)	

   As always, be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

7. Let (N_1, e_1) and (N_2, e_2) be the RSA public keys for Alice and Bob, respectively. Suppose however that by coincidence, N_1 and N_2 are not coprime. Can you compute the decryption exponents d_1 and d_2 belonging to Alice and Bob, respectively? Why or why not? Prove your answer.

1. Answer the following questions regarding $\mathbf{Z}_{23}^*$.

(a) What are the elements of $\mathbf{Z}_{23}^*$? List all of them.

23 is prime. Thus, every number between 1 & 22, inclusive, is in $\mathbb{Z}_{23}^*$ since it is coprime with 23.

$\mathbb{Z}_{23}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22\}$

(b) What is the order of this group?

The order of a group is its size. So, the order of $\mathbb{Z}_{23}^* = |\mathbb{Z}_{23}^*| = 22$.

(c) What is the order of 2?

(d) What is the order of 5?

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$2^i \bmod 23$	2	4	8	16	9	18	13	3	6	12	1											
$5^i \bmod 23$	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1

Thus, the order of 2 and 5 are 11 and 22, respectively.

(e) Is $\mathbf{Z}_{23}^*$ cyclic? If your answer is "yes," provide a generator. If your answer is "no," explain your answer.

Yes. 5 is a generator since its order is the size of the group.

2. Prove that the hardness of the DDH problem implies the hardness of the CDH problem. Use the definitions of these problems as specified in the lecture slides.

We show that, given an adversary A solving CDH, we can construct an adversary B solving DDH with comparable advantage value and resources.

Let $\mathbb{G}$ be a cyclic group generated by g of order m.

CONSTRUCTION: Adversary $B(X, Y, Z)$:

$z' \xleftarrow{\$} A(X, Y)$

If $z' = z$ then return 1 else return 0.

ANALYSIS: Let b be the bit in Game $DDH_{\mathbb{G},g}$.

Consider $\Pr[DDH_{\mathbb{G},g}(B) \Rightarrow true] = \Pr[DDH_{\mathbb{G},g}(B) \Rightarrow true \mid b=1]\Pr[b=1] + \Pr[DDH_{\mathbb{G},g}(B) \Rightarrow true \mid b=0]\Pr[b=0]$ ⊛

Case $b=1$: When $b=1$, the value z given to B is g^{xy} if $X=g^x$ and $Y=g^y$.

So, $\Pr[DDH_{\mathbb{G},g}(B) \Rightarrow true \mid b=1] = Adv^{cdh}_{\mathbb{G},g}(A)$. ①

Case $b=0$: When $b=0$, the value z given to B is chosen at random from $\mathbb{G}$.

The probability that $z' = g^{xy}$ would happen to be equal to z is $\frac{1}{m}$ since $m = |\mathbb{G}|$.

Thus, $\Pr[DDH_{\mathbb{G},g}(B) \Rightarrow true \mid b=0] = 1 - \Pr[DDH_{\mathbb{G},g}(B) \Rightarrow false \mid b=0]$

$= 1 - \Pr[z' = z \mid b=0]$ // when $z' \neq z$, B returns 1 even though $b=0$.

$= 1 - \frac{1}{m}$ ②

Substituting ① & ② into ⊛, we obtain

$\Pr[DDH_{\mathbb{G},g}(B) \Rightarrow true] = \left(Adv^{cdh}_{\mathbb{G},g}(A)\right)\frac{1}{2} + \left(1 - \frac{1}{m}\right)\frac{1}{2}$, which leads to

$$Adv^{ddh}_{\mathbb{G},g}(B) = 2\left[\left(Adv^{cdh}_{\mathbb{G},g}(A)\right)\frac{1}{2} + \left(1 - \frac{1}{m}\right)\frac{1}{2}\right] - 1$$

$$= Adv^{cdh}_{\mathbb{G},g}(A) + 1 - \frac{1}{m} - 1$$

$$= Adv^{cdh}_{\mathbb{G},g}(A) - \frac{1}{m}$$

Thus, $Adv^{cdh}_{\mathbb{G},g}(A) \leq Adv^{ddh}_{\mathbb{G},g}(B) + \frac{1}{m}$.

If DDH is hard, $Adv^{ddh}_{\mathbb{G},g}(B)$ is small.

Thus, for large groups, CDH would be hard as well.

RESOURCES: B runs in essentially the same amount of time as A.

Neither A nor B make any oracle queries.

3. Let p be an odd prime, and let G be $\mathbf{Z}_p^*$. Suppose g is a generator of $\mathbf{Z}_p^*$ but oddly enough is kept secret. Let $x \in \mathbf{Z}_{p-1}$, and let $y = g^x \bmod p$. Given inputs p, x, and y, is it possible to compute g in polynomial time in the size of the inputs? Prove your answer. You may refer to algorithms we studied in class by name without explicitly defining how they work.

Since p is prime, $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$, so $|\mathbb{Z}_p^*| = p-1$.

Thus, MOD-INV$(x, p-1)$ yields x^{-1} in $\mathbb{Z}_{\phi(p)}^* = \mathbb{Z}_{p-1}^*$

We can compute MOD-EXP(y, x^{-1}, p) to obtain

$$y^{x^{-1}} \equiv (g^x)^{x^{-1}} \pmod p$$
$$\equiv g \pmod p.$$

In summary, the algorithm works as follows:

On input x, y, p,
$x^{-1} \leftarrow$ MOD-INV$(x, p-1)$
Return MOD-EXP(y, x^{-1}, p)

Let n be the size of p.
The 1st line takes quadratic time in n.
The 2nd line takes cubic time in n.

Thus, we can compute g in cubic time in n.

4. Compute $19^{571500000}$ mod 77 by hand. Show your work and justify all the steps in your computation.

Notice that $77 = 7 * 11$. Both 7 & 11 are prime.
Thus, $|\mathbb{Z}_{77}^*| = \phi(77) = (7-1)(11-1) = 6 * 10 = 60$.

Therefore,
$$19^{571500000} \equiv 19^{571500000 \bmod 60} \pmod{77}$$
$$\equiv 19^0 \pmod{77}$$
$$\equiv 1 \pmod{77}$$

5. Prove that DDH is easy in $\mathbf{Z}_p^*$ when p is an odd prime. Here, you may use without proof, the properties we studied in class about the Legendre (equivalently in this context, the Jacobi) symbol.

Let g be a generator of $\mathbb{Z}_p^*$.
We know the following facts from class:

① In this case, the Jacobi symbol can be computed as $J_p(x) = x^{\frac{p-1}{2}} \pmod p$.

② $\forall a,b \in \mathbb{Z}_{p-1}$, $J_p(g^{ab}) = 1$ iff $J_p(g^a) = 1$ or $J_p(g^b) = 1$.

We can then solve DDH using the following algorithm:

CONSTRUCTION:

Algorithm $A(X, Y, Z)$:
(1) $J_1 \leftarrow X^{\frac{p-1}{2}} \mod p$
(2) $J_2 \leftarrow Y^{\frac{p-1}{2}} \mod p$
(3) $J_3 \leftarrow Z^{\frac{p-1}{2}} \mod p$
(4) If $(J_1, J_2, J_3) \in \{(1,1,1), (1,-1,1), (-1,1,1), (-1,-1,-1)\}$
(5) then return 1 else return 0.

ANALYSIS: Let b be the bit in Game $DDH_{G,g}$.

Consider $\Pr[DDH_{G,g}(B) \Rightarrow true] = \Pr[DDH_{G,g}(B) \Rightarrow true \mid b=1]\Pr[b=1] + \Pr[DDH_{G,g}(B) \Rightarrow true \mid b=0]\Pr[b=0]$ ★

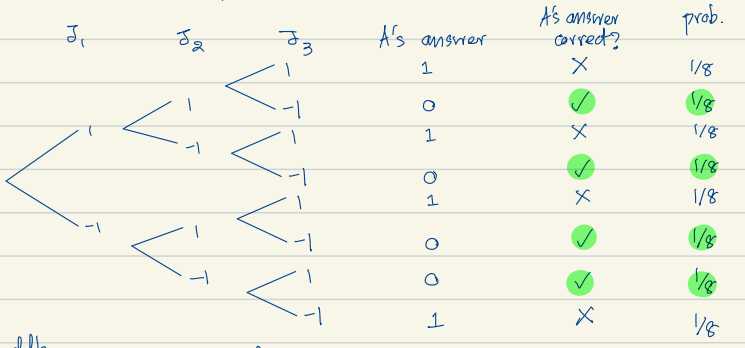
Case $b=1$: Let $g^x = X$ and $g^y = Y$. Then, $Z = g^{xy}$ in this case.
Due to fact ②, we know that the following table holds:

J_1	J_2	J_3
1	1	1
1	-1	1
-1	1	1
-1	-1	-1

The triples from this table are the triples in the set on line (4).

Since $Z = g^{xy}$, for each row in the table, the opposite value of J_3 is impossible.
Thus, A always answer 1, which is the correct answer.
Therefore, $\Pr[DDH_{G,g}(A) \Rightarrow true \mid b=1] = 1$ ①

Case $b=0$: In this case, Z is chosen at random from G.
We draw the probability tree associated with this scenario. Note that all the branches are associated with probability $\frac{1}{2}$.



Thus, $\Pr[DDH_{G,g}(A) \Rightarrow true \mid b=0] = (\frac{1}{8}) * 4 = \frac{1}{2}$. ②

Thus, $Adv^{ddh}_{G,g}(A) = 2 * \Pr[DDH_{G,g}(A) \Rightarrow true] - 1$
$= 2 * [1(\frac{1}{2}) + \frac{1}{2}(\frac{1}{2})] - 1 = 1 + \frac{1}{2} - 1 = \frac{1}{2}$ from ★, ①, ②.

RESOURCES: Algorithm A take cubic time in the size of p due to modular exponentiation.

6. Suppose DDH is hard for a group G. Consider the ElGamal encryption scheme $(\mathsf{KG}, \mathcal{E}, \mathcal{D})$ based on G as studied in class and recalled here for your convenience. (In the description, g is a generator of G, and m is its order.) Is this scheme secure under IND-CCA? Prove your answer.

Alg KG	**Alg** $\mathcal{E}_X(M)$	**Alg** $\mathcal{D}_x(Y, W)$
$x \xleftarrow{\$} \mathbf{Z}_m$	$y \xleftarrow{\$} \mathbf{Z}_m$; $Y \leftarrow g^y$	$K \leftarrow Y^x$
$X \leftarrow g^x$	$K \leftarrow X^y$	$M \leftarrow W \cdot K^{-1}$
Return (X, x)	$W \leftarrow K \cdot M$	Return M
	Return (Y, W)	

As always, be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

No, if is not.
We assume here that $m > 2$. We attack the scheme as follows.

CONSTRUCTION: Adversary $A^{Enc, Dec}(X)$:

(1) $(Y, W) \xleftarrow{\$} Enc(1, g)$
(2) $W' \leftarrow W \cdot g$
(3) $M \leftarrow Dec(Y, W')$
(4) If $M \cdot g^{-1} \equiv 1$ then return 0 else return 1

ANALYSIS: Consider $\Pr[Exp^{ind\text{-}cca}_{ElGamal}(A) \Rightarrow true] = \Pr[Exp^{ind\text{-}cca}_{ElGamal}(A) \Rightarrow true \mid b=0]\Pr[b=0] + \Pr[Exp^{ind\text{-}cca}_{ElGamal}(A) \Rightarrow true \mid b=1]\Pr[b=1]$ ★

Case $b=0$: (1) is encrypted. Let $g^x = X$. Then, $W = Y^x \cdot (1)$ from the encryption alg.
So, $W' = Y^x \cdot g \neq W$.
So, on line (3), the decryption oracle will return $M = W' \cdot K^{-1} = Y^x \cdot g \cdot (Y^x)^{-1} = g$.
Thus, $M \cdot g^{-1} = g \cdot g^{-1} = 1$, and A returns 0, which is correct.
So, $\Pr[Exp^{ind\text{-}cca}_{ElGamal}(A) \Rightarrow true \mid b=0] = 1$. ①

Case $b=1$: (g) is encrypted. Let $g^x = X$. Then, $W = Y^x \cdot g$ from the encryption alg.
So, $W' = Y^x \cdot g^2 \neq W$.
So, on line (3), the decryption oracle will return $M = W' \cdot K^{-1} = Y^x \cdot g^2 \cdot (Y^x)^{-1} = g^2$.
Thus, $M \cdot g^{-1} = g^2 \cdot g^{-1} = g \neq 1$, and A returns 1, which is correct.

So, $\Pr[Exp^{ind\text{-}cca}_{ElGamal}(A) \Rightarrow true \mid b=1] = 1$. ②

Substituting ★, ①, ② to compute $Adv^{ind\text{-}cca}_{ElGamal}(A)$, we get

$$Adv^{ind\text{-}cca}_{ElGamal}(A) = 2\left[1\left(\tfrac{1}{2}\right) + 1\left(\tfrac{1}{2}\right)\right] - 1 = 1.$$

RESOURCES: Line (1) takes however much time to perform one encryption oracle call.
" (2) takes however much time to perform 1 group operation.
" (3) takes however much time to perform one decryption oracle call.
For " (4), since the order of the group is known, A can easily compute g^{-1} using the extended Euclidean algorithm (MOD-INV(g, m)).

$q_e = 1$, μ_e = the size of 1 group element
$q_d = 1$, μ_d = the size of 2 group elements

7. Let (N_1, e_1) and (N_2, e_2) be the RSA public keys for Alice and Bob, respectively. Suppose however that by coincidence, N_1 and N_2 are not coprime. Can you compute the decryption exponents d_1 and d_2 belonging to Alice and Bob, respectively? Why or why not? Prove your answer.

Yes, we can compute d_1, d_2 as follows:

Algorithm $A(N_1, N_2, e_1, e_2)$:

(1) $p \leftarrow \gcd(N_1, N_2)$
(2) $q_1 \leftarrow N_1 / p$ // / denotes integer division
(3) $q_2 \leftarrow N_2 / p$
(4) $\phi_1 \leftarrow (p-1)(q_1-1)$
(5) $\phi_2 \leftarrow (p-1)(q_2-1)$
(6) $d_1 \leftarrow$ MOD-INV(e_1, ϕ_1)
(7) $d_2 \leftarrow$ MOD-INV(e_2, ϕ_2)

Since N_1, N_2 aren't coprime, $p \neq 1$.
Since N_1, N_2 are RSA moduli, they must be products of 2 primes, one of which is p.
In class, we showed, using counting arguments, that $\phi(N_1) = (p-1)(q_1-1)$ if $N_1 = p \cdot q_1$. This applies to lines (4), (5).

Since e_1, d_1 are inverses of each other in $\mathbb{Z}^*_{\phi(N_1)} = \mathbb{Z}^*_{(p-1)(q_1-1)}$, we can use the extended Euclidean algorithm to compute $d_1 = e_1^{-1} \pmod{\phi(N_1)}$. Similarly for e_2 & d_2.

Algorithm A runs in polynomial time. In particular, each operation that A performs take quadratic time.