CMSC/Math 456: Cryptography (Fall 2022)

Lecture 11

Daniel Gottesman

Administrative

Problem 3a (on PS#4): N is now 465.

Regrade policy: Regrade requests should be submitted at most 1 week after both the solutions and the grades for the assignment have been released.
For Problem sets #1 and #2, you can still submit regrade requests until 1 week from today.

Midterm: Thursday, Oct. 20 (2 weeks from Thursday)

- In class
- Open book (including textbook), no electronic devices
- Will cover classical cryptographic, private key encryption, and public key encryption and key exchange, including all topics discussed under those general subjects (such as number theory).
- Those with accommodations remember to book with ADS.

This class is being recorded

Diffie-Hellman Security Idea

In Diffie-Hellman, Alice and Bob must perform modular exponentiation: Alice announces $A = g^a \bmod p$ and Bob announces $B = g^b \bmod p$ for secret a and b chosen by Alice and Bob respectively and not shared with each other or Eve. Then they do another pair of modular exponentiations B^a and A^b to calculate the key.

- Alice and Bob must compute modular exponentials, which can be done in polynomial time in the *length* of p, g.

Eve can break Diffie-Hellman if she can calculate the discrete log for (g,p): That is, if given y, she can find x such that $g^x = y \bmod p$.

- So, for security, we need that calculating the discrete log is hard.

We are studying modular arithmetic to understand the difficulty of discrete log.

Group Theory

Definition: A group (G, *) is a set G of elements along with a binary operation $* : G \times G \to G$ with the following properties:

1. Closure: $g * h \in G$ when $g, h \in G$.
2. Associativity: $\forall g, h, k \in G, (g * h) * k = g * (h * k)$.
3. Identity: $\exists e \in G$ such that $\forall g \in G, e * g = g * e = g$.
4. Inverses: $\forall g \in G, \exists g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

A subgroup H of G, written $H \leq G$ is a subset of G which is also a group. The order $|G|$ of a finite group G is the number of elements.

A set S generates a group G if all elements of G can be written as products of elements of S. A group that can be generated by just one element is cyclic.

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

This class is being recorded

Cyclic Subgroups of $\mathbb{Z}_N^*$

What are the possible orders of an element under modular exponentiation?

Let $g \in \mathbb{Z}_N^*$ and define $\langle g \rangle = \{g^a \in \mathbb{Z}_N^*\}$. $\langle g \rangle$ is the cyclic subgroup of $\mathbb{Z}_N^*$ generated by g.

> (Why is it a subgroup? $g^a g^b = g^{a+b}$, so it is closed, and $g \cdot g^{\mathrm{ord}(g)-1} = 1$, so $g^{-1} = g^{\mathrm{ord}(g)-1} \in \langle g \rangle$, so $\langle g \rangle$ has inverses since $(g^a)^{-1} = (g^{-1})^a$.)

By Lagrange's Theorem, $\mathrm{ord}(g) = |\langle g \rangle|$ divides $|\mathbb{Z}_N^*|$. This tells us the possible values of the order of g: the factors of $|\mathbb{Z}_N^*|$.

> When N is prime, then everything smaller than N is relatively prime to it, so $|\mathbb{Z}_N^*| = N - 1$.

What is $|\mathbb{Z}_N^*|$ when N is not prime?

Euler Totient Function

Let $\varphi(N) = \mathbb{Z}_N^*$. That is, $\varphi(N)$ is equal to the number of positive integers $j \leq N$ such that $\gcd(j, N) = 1$. (Euler's totient function)

Examples:

When p prime, $\varphi(p) = p - 1$

$\varphi(4) = 2$: 1 and 3 are relatively prime to 4.

$\varphi(6) = 2$: 1 and 5 are relatively prime to 6.

$\varphi(10) = 4$: 1, 3, 7, and 9 are relatively prime to 10.

$\varphi(21) = 12$: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, and 20 are relatively prime to 21.

$\varphi(24) = 8$: 1, 5, 7, 11, 13, 17, 19, and 23 are relatively prime to 24.

Totient for Product of Two Primes

Let $N = pq$ for p and q prime, $p < q$. What is $\varphi(N)$?

List numbers *not* relatively prime to N:

Divisible by p: p, 2p, 3p, 4p, …, (q-1)p, pq = N

There are exactly q numbers on this list.

Divisible by q: q, 2q, 3q, 4q, …, (p-1)q, pq = N

There are exactly p numbers on this list.

But: Some numbers appear on both lists.

To appear on both lists, the number must be divisible by both p and q. Only N qualifies.

Thus: # not relatively prime = $(q-1) + (p-1) + 1 = p + q - 1$.

$$\varphi(N) = N - (p + q - 1) = (p-1)(q-1)$$

General Formula for Totient

Theorem: If $N = \prod_i p_i^{e_i}$ is the prime factorization of N (so every p_i is prime), then

$$\varphi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$$

In general, numbers with fewer factors have larger values of $\varphi(N)$.

Euler-Fermat Theorem

Putting together our deductions about the order of numbers for modular exponentiation with the rules for $\varphi(N)$, we get the following theorem:

Euler-Fermat Theorem: $x^{\varphi(N)} = 1 \bmod N$ for any integers x, N with $\gcd(x, N) = 1$.

Corollary (Fermat's Little Theorem): $x^p = x \bmod p$ for any integer x and any prime p.

Proof: Since the order divides $|\mathbb{Z}_N^*| = \varphi(N)$,

$$x^{\varphi(N)} = (x^{\mathrm{ord}(x)})^{\varphi(N)/\mathrm{ord}(x)} = 1^{\varphi(N)/\mathrm{ord}(x)} = 1 \bmod N$$

If we want to have elements of a large order, our best bet is to work modulo a prime.

Euler's Theorem Examples

Example 1:

N = 10, $\varphi(10) = 4$

$3^4 = 81 = 1 \text{ mod } 10, 7^4 = 2401 = 1 \text{ mod } 10$

Example 2:

N = 21, $\varphi(21) = 12$

$5^6 = 15{,}625 = 1 \text{ mod } 21, 11^6 = 1{,}771{,}561 = 1 \text{ mod } 21$

Actually, in $\mathbb{Z}_{21}^*$, the highest order is 6. But $6 \mid 12$, so the Euler-Fermat theorem still applies.

Modulo a Prime

But … the theorem only says that when p is prime, the order *divides* p-1, not that it *is* p-1.

Modulo a Prime

But … the theorem only says that when p is prime, the order *divides* p-1, not that it *is* p-1.

Recall the example from last time. Mod 11, it is actually the case that ord(7) = 10. This implies that $\mathbb{Z}_{11}^*$ is cyclic, and 7 is a generator.

Theorem: When p is prime, $\mathbb{Z}_p^*$ is cyclic.

$$7^1 = 7 \bmod 11$$
$$7^2 = 5 \bmod 11$$
$$7^3 = 2 \bmod 11$$
$$7^4 = 3 \bmod 11$$
$$7^5 = 10 \bmod 11$$
$$7^6 = 4 \bmod 11$$
$$7^7 = 6 \bmod 11$$
$$7^8 = 9 \bmod 11$$
$$7^9 = 8 \bmod 11$$
$$7^{10} = 1 \bmod 11$$

ord(7) = 10

Modulo a Prime

But … the theorem only says that when p is prime, the order *divides* p-1, not that it *is* p-1.

Recall the example from last time. Mod 11, it is actually the case that ord(7) = 10. This implies that $\mathbb{Z}_{11}^*$ is cyclic, and 7 is a generator.

Theorem: When p is prime, $\mathbb{Z}_p^*$ is cyclic.

By picking a large prime base, we could have a high order element … but how many elements actually have order p-1?

$$7^1 = 7 \bmod 11$$
$$7^2 = 5 \bmod 11$$
$$7^3 = 2 \bmod 11$$
$$7^4 = 3 \bmod 11$$
$$7^5 = 10 \bmod 11$$
$$7^6 = 4 \bmod 11$$
$$7^7 = 6 \bmod 11$$
$$7^8 = 9 \bmod 11$$
$$7^9 = 8 \bmod 11$$
$$7^{10} = 1 \bmod 11$$

ord(7) = 10

This class is being recorded

Distribution of Orders

Given prime p and generator g_0 for $\mathbb{Z}_p^*$, which $g \in \mathbb{Z}_p^*$ have order p-1 and which have a lower order?

Distribution of Orders

Given prime p and generator g_0 for $\mathbb{Z}_p^*$, which $g \in \mathbb{Z}_p^*$ have order p-1 and which have a lower order?

Suppose $g = g_0^j$. Then

$$g^r = (g_0^j)^r = g_0^{jr} = g_0^{r'} \bmod p$$

when $r' = jr \bmod (p-1)$ since $\mathrm{ord}(g_0) = p - 1$.

That is, $r' = 0$ if $(p-1) \mid jr$.

Distribution of Orders

Given prime p and generator g_0 for $\mathbb{Z}_p^*$, which $g \in \mathbb{Z}_p^*$ have order p-1 and which have a lower order?

Suppose $g = g_0^j$. Then

$$g^r = (g_0^j)^r = g_0^{jr} = g_0^{r'} \bmod p$$

when $r' = jr \bmod (p-1)$ since $\mathrm{ord}(g_0) = p - 1$.

That is, $r' = 0$ if $(p-1) \mid jr$.

If $\gcd(j, p-1) = 1$, then $(p-1) \mid jr$ only when $(p-1) \mid r$.
Therefore, if $\gcd(j, p-1) = 1$, $\mathrm{ord}(g_0^j) = p - 1$.

Otherwise, $\mathrm{ord}(g_0^j)$ is smaller. In particular,

$$\mathrm{ord}(g_0^j) = \frac{p-1}{\gcd(j, p-1)}$$

Order Distribution Example

Let's see how this works with p=11.

Since 1, 3, 7, and 9 are relatively prime to p-1 = 10, we conclude the possible generators of $\mathbb{Z}_{11}^*$ are 7, 2, 6, and 8.

We can also conclude that 5, 3, 4, and 9 have order 5 since they are even powers of 7: e.g.,

$$3^5 = 243 \bmod 11 = 1 \bmod 11$$

And $10 = 7^5 \bmod 11$ has order 2:

$$10^2 = 100 \bmod 11 = 1 \bmod 11$$

$7^1 = 7 \bmod 11$

$7^2 = 5 \bmod 11$

$7^3 = 2 \bmod 11$

$7^4 = 3 \bmod 11$

$7^5 = 10 \bmod 11$

$7^6 = 4 \bmod 11$

$7^7 = 6 \bmod 11$

$7^8 = 9 \bmod 11$

$7^9 = 8 \bmod 11$

$7^{10} = 1 \bmod 11$

ord(7) = 10

Subgroups of $\mathbb{Z}_p^*$

The group $\mathbb{Z}_p^*$ can therefore be generated by any of the $\varphi(p-1)$ elements of the form g_0^j for $\gcd(j, p-1) = 1$.

We can also consider subgroups of $\mathbb{Z}_p^*$ generated by g_0^j for $\gcd(j, p-1) \neq 1$.

In particular, the subgroup $\langle g_0^j \rangle$ has order $(p-1)/\gcd(j, p-1)$.

For the $\mathbb{Z}_{11}^*$ example, we get two non-trivial subgroups:

$\langle 5 \rangle = \{1,3,4,5,9\}$ of order 5

$\langle 10 \rangle = \{1,10\}$ of order 2.

There is a subgroup corresponding to any factor of p-1.

This class is being recorded

Other Groups

The same arguments apply to any finite cyclic group G: There are $\varphi(|G|)$ possible generators and other elements will generate cyclic subgroups whose order is a factor of $|G|$.

Note that when $|G|$ is prime, then *all* non-identity elements are generators of the group. (And a group of prime order is automatically cyclic as well.)

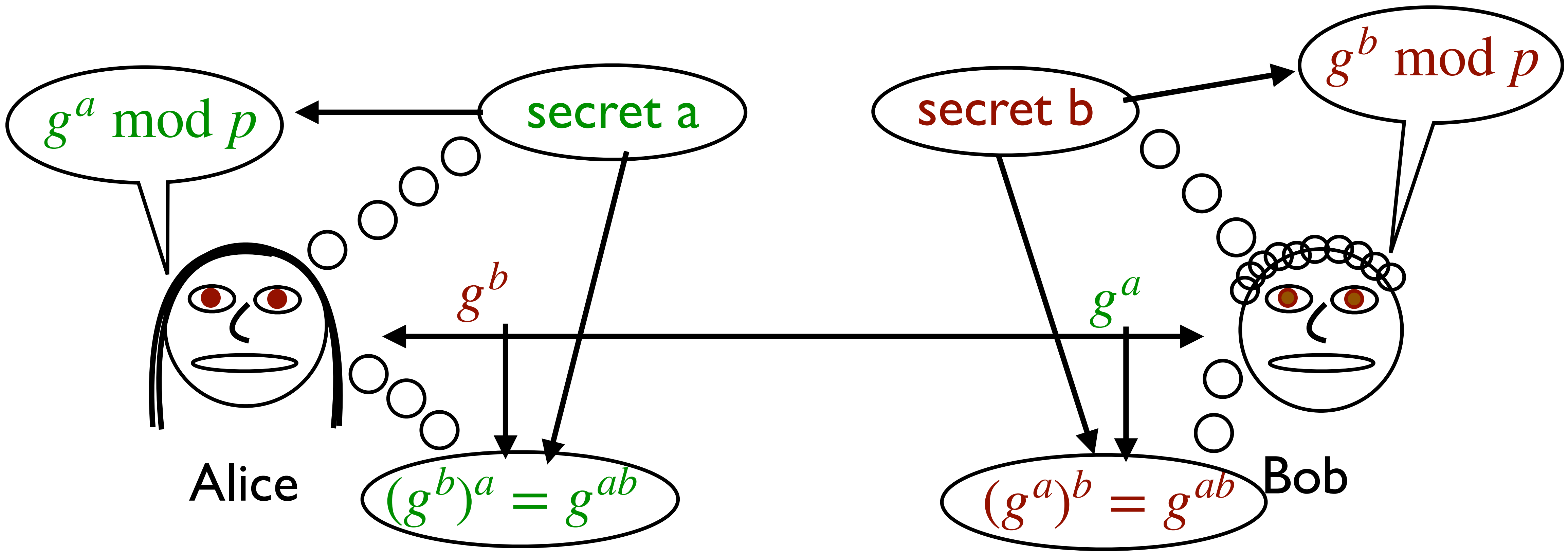
Unfortunately, for any prime $p > 3$, $|\mathbb{Z}_p^*| = p - 1$ is not prime, so we are left with the case that only some elements are generators.

Also note that when N is not prime, $\mathbb{Z}_N^*$ might not be cyclic, although it is always a group.

For instance, in $\mathbb{Z}_8^* = \{1,3,5,7\}$, all three non-zero elements 3, 5, and 7 have order 2 and therefore only generate order 2 subgroups. $\mathbb{Z}_{21}^*$ is another example.

This class is being recorded

Application to Diffie-Hellman

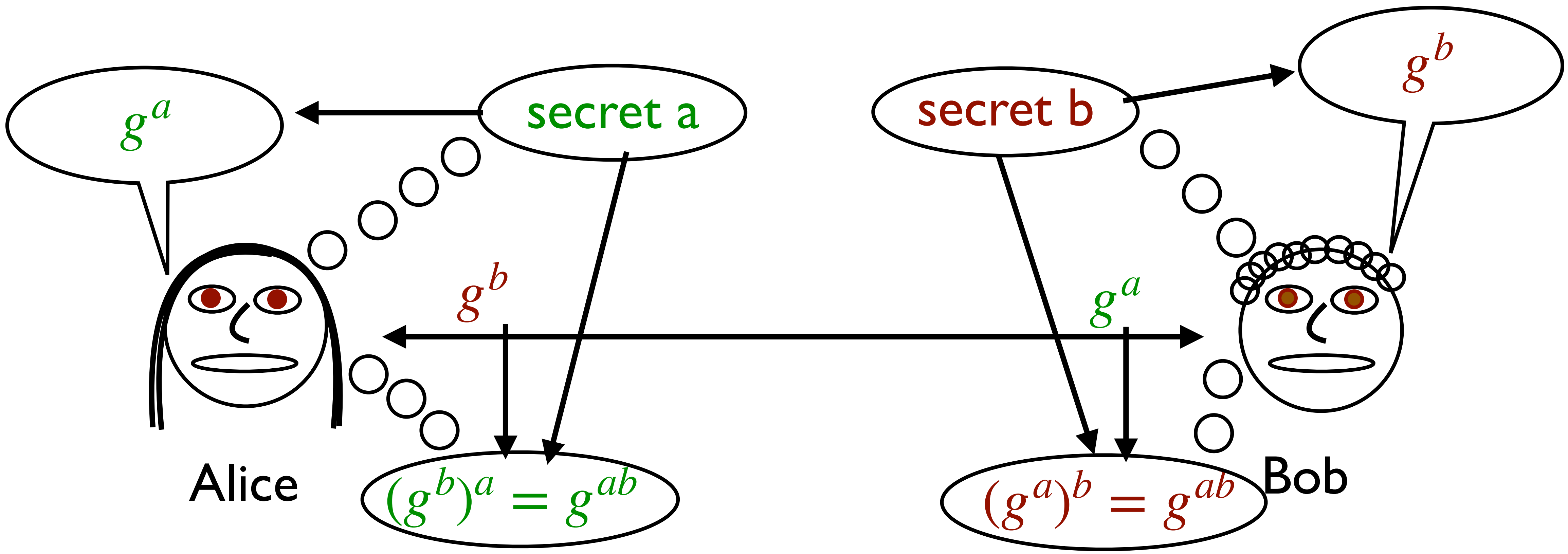


In order to have some hope that Diffie-Hellman is secure, we want:

- To pick a large prime p
- To have $\varphi(p-1)$ large so it is not too hard to find elements with high order
- To actually pick a g with high order

Diffie-Hellman with Groups

Diffie-Hellman also works when g is drawn from a group G.



Alice and Bob must first agree on the group G and the element g. G is cyclic and $G = \langle g \rangle$.

Again, they can use standardized values for g and G.

Elliptic curves are common; they allow smaller groups than modular arithmetic.

This class is being recorded

Bad Primes for Discrete Log

We need to make an additional constraint on the choice of prime p for Diffie-Hellman. When p-1 is itself a product of small primes, there is a fast algorithm for discrete log (Pohlig-Hellman).

The attack relies on the Chinese remainder theorem:

Theorem: Let N = ab, with a and b relatively prime. Given any pair of non-negative integers (x_a, x_b), with $x_a < a$ and $x_b < b$, there exists a unique non-negative integer $x < N$ such that $x = x_a \bmod a$ and $x = x_b \bmod b$. There is an efficient algorithm to compute x.

Algorithm: Using Euclid's algorithm, compute X and Y such that $aX + bY = 1$.

Then $x = x_b aX + x_a bY$.

Why? $bY = 1 - aX$, so $x = (x_b X - x_a X)a + x_a$, so $x = x_a \bmod a$.

This class is being recorded

Chinese Remainder Theorem

Example:

Suppose we want to find an x such that

$$x = 5 \bmod 14$$
$$x = 3 \bmod 5$$

We could apply Euclid's algorithm to see that

$$3 * 5 - 1 * 14 = 1$$

We then have

$$x = 5 * 15 - 3 * 14 = 33$$