CMSC/Math 456: Cryptography (Fall 2023)

Lecture 11

Daniel Gottesman

Administrative

Problem set #5 due Thursday.

Midterm: Thursday, Oct. 19 (2 weeks from Thursday)

- In class
- Open book (including textbook), no electronic devices
- Will cover classical cryptographic, private key encryption, modular arithmetic, and public key exchange (probably not public key encryption).
- Those with accommodations remember to book with ADS.

Order Under Modular Exponentiation

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

Recall that $\mathbb{Z}_N^*$, the set of elements relatively prime to N, forms a group under multiplication, and that $\langle g \rangle$, the powers of g mod N, is a subgroup of $\mathbb{Z}_N^*$.

By Lagrange's Theorem, $\text{ord}(g) = |\langle g \rangle|$ 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?

This class is being recorded

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:

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

This class is being recorded

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.

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.

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.

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.

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:

This class is being recorded

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.

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.

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.

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.

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 = $(q-1) + (p-1) + 1 = p + q - 1$.

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

This class is being recorded

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.

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 $|\mathbb{Z}_N^*| = \varphi(N)$,

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

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, or failing that, a product of 2 primes.

Euler's Theorem Examples

Example 1:

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

$3^4 = 81 = 1 \bmod 10$

$7^4 = 2401 = 1 \bmod 10$

Euler's Theorem Examples

Example 1:

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

$$3^4 = 81 = 1 \bmod 10$$

$$7^4 = 2401 = 1 \bmod 10$$

Example 2:

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

$$5^6 = 15{,}625 = 1 \bmod 21$$

$$11^6 = 1{,}771{,}561 = 1 \bmod 21$$

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

When p is prime, the theorems we have only say that the order *divides* p-1, not that it *is* p-1.

Modulo a Prime

When p is prime, the theorems we have only say that the order *divides* p-1, not that it *is* p-1.

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

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

ord(7) = 10

Modulo a Prime

When p is prime, the theorems we have only say that the order *divides* p-1, not that it *is* p-1.

Recall the example 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.

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

ord(7) = 10

Modulo a Prime

When p is prime, the theorems we have only say that the order *divides* p-1, not that it *is* p-1.

Recall the example 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?

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

ord(7) = 10

Number of Generators

Recall: if $y = x^a \bmod N$ and $r = \mathrm{ord}(x)$, then

$$\mathrm{ord}(y) = \frac{r}{\gcd(a, r)}$$

Thus, if g_0 has order r, then g_0^j also has order r if $\gcd(j, r) = 1$.

In particular, if g_0 is a generator of $\mathbb{Z}_p^*$ (p prime), then g_0^j is also a generator if $\gcd(j, p-1) = 1$.

> Note: These are the *only* generators: every element of $\mathbb{Z}_p^*$ can be written as g_0^j for some j because g_0 is a generator, but if $\gcd(j, p-1) \neq 1$, then $\mathrm{ord}(g_0^j) < p - 1$.

The group $\mathbb{Z}_p^*$ has $\varphi(p-1)$ generators.

Order Distribution Example

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

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

ord(7) = 10

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.

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

ord(7) = 10

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.,

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

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

ord(7) = 10

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 $\mathbb{Z}_p^*$

It is also interesting to look at 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.

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.

Multiple Moduli

We can convert back and forth between integer type and modular type. Can we convert between different moduli?

Example:

Suppose we know that $x = 3 \bmod 5$. What is $x \bmod 14$?

Multiple Moduli

We can convert back and forth between integer type and modular type. Can we convert between different moduli?

Example:

Suppose we know that $x = 3 \bmod 5$. What is $x \bmod 14$?

Answer:

It's not unique.

Certainly, x=3, 8, 13 all work.

Multiple Moduli

We can convert back and forth between integer type and modular type. Can we convert between different moduli?

Example:

Suppose we know that $x = 3 \bmod 5$. What is $x \bmod 14$?

Answer:

It's not unique.

Certainly, x=3, 8, 13 all work.

But the integer x=18 is also 3 mod 5, and $18 = 4 \bmod 14$. So 4 also seems possible.

Multiple Moduli

We can convert back and forth between integer type and modular type. Can we convert between different moduli?

Example:

Suppose we know that $x = 3 \bmod 5$. What is $x \bmod 14$?

Answer:

It's not unique.

Certainly, x=3, 8, 13 all work.

But the integer x=18 is also 3 mod 5, and $18 = 4 \bmod 14$.
So 4 also seems possible.

Actually, it could be anything!

Chinese Remainder Theorem

Chinese Remainder 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.

$x = x_a \bmod a$ $\qquad$ $x = x_b \bmod b$

Unique $x \bmod N = ab$

This class is being recorded

Reasoning

(Assume $a<b$ and $\gcd(a, b) = 1$.)

Mod a	Mod N=ab	Mod b

Reasoning

(Assume a<b and $\gcd(a, b) = 1$.)

Mod a	Mod N=ab	Mod b
$x = x_a \bmod a$	x_a	x_a

Reasoning

(Assume a<b and $\gcd(a, b) = 1$.)

Mod a	Mod N=ab	Mod b
$x = x_a \bmod a$	x_a	x_a
	$x_a + a$	$x_a + a \bmod b$

Reasoning

(Assume a<b and $\gcd(a, b) = 1$.)

Mod a	Mod N=ab	Mod b
$x = x_a \bmod a$	x_a	x_a
	$x_a + a$	$x_a + a \bmod b$
	$x_a + 2a$	$x_a + 2a \bmod b$

Reasoning

(Assume a<b and $\gcd(a, b) = 1$.)

Mod a	Mod N=ab	Mod b
$x = x_a \bmod a$	x_a	x_a
	$x_a + a$	$x_a + a \bmod b$
	$x_a + 2a$	$x_a + 2a \bmod b$
	$\vdots$	
	$x_a + ma$	$x_a + ma + nb = x_b$

with n chosen so that $x_a + ma + nb < b$.

Reasoning

(Assume $a<b$ and $\gcd(a, b) = 1$.)

Mod a	Mod N=ab	Mod b
$x = x_a \bmod a$	x_a	x_a
	$x_a + a$	$x_a + a \bmod b$
	$x_a + 2a$	$x_a + 2a \bmod b$
	$\vdots$	
	$x_a + ma$	$x_a + ma + nb = x_b$

with n chosen so that $x_a + ma + nb < b$.

We need to find m and n so that $ma + nb = x_b - x_a$.

Reasoning

(Assume a<b and $\gcd(a, b) = 1$.)

Mod a	Mod N=ab	Mod b
$x = x_a \bmod a$	x_a	x_a
	$x_a + a$	$x_a + a \bmod b$
	$x_a + 2a$	$x_a + 2a \bmod b$
	$\vdots$	
	$x_a + ma$	$x_a + ma + nb = x_b$

with n chosen so that $x_a + ma + nb < b$.

We need to find m and n so that $ma + nb = x_b - x_a$.

Euclid's algorithm gives X and Y with $aX + bY = 1$. Multiply by $(x_b - x_a)$.

Chinese Remainder Theorem Alg.

Algorithm:

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

2. Let $m = X(x_b - x_a), n = Y(x_b - x_a)$.

3. Let $x = x_a + ma = x_a(1 - aX) + x_b aX$.

Chinese Remainder Theorem Alg.

Algorithm:

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

2. Let $m = X(x_b - x_a), n = Y(x_b - x_a)$.

3. Let $x = x_a + ma = x_a(1 - aX) + x_b aX$. ⇨ $x = x_a \bmod a$

This class is being recorded

Chinese Remainder Theorem Alg.

Algorithm:

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

2. Let $m = X(x_b - x_a), n = Y(x_b - x_a)$.

3. Let $x = x_a + ma = x_a(1 - aX) + x_b aX$. ⇒ $x = x_a \bmod a$

Note that $1 - aX = bY$ and $aX = 1 - bY$, so

$$x = x_a bY + x_b(1 - bY) = x_b + nb \quad \Rightarrow \quad x = x_b \bmod b$$

Chinese Remainder Theorem Alg.

Algorithm:

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

2. Let $m = X(x_b - x_a), n = Y(x_b - x_a)$.

3. Let $x = x_a + ma = x_a(1 - aX) + x_b aX$. ⇒ $x = x_a \bmod a$

Note that $1 - aX = bY$ and $aX = 1 - bY$, so

$$x = x_a bY + x_b(1 - bY) = x_b + nb$$ ⇒ $x = x_b \bmod b$

Alternative more symmetric formula:

$$x = x_b aX + x_a bY$$

This class is being recorded

Chinese Remainder Theorem

Example:

Suppose we want to find an x such that

$$x = 5 \bmod 14 \qquad x_a = 5,\ a = 14$$

$$x = 3 \bmod 5 \qquad x_b = 3,\ b = 5$$

We could apply Euclid's algorithm to see that

$$3 * 5 - 1 * 14 = 1 \qquad X = -1,\ Y = 3$$

We then have

$$x = 3 * 14 * (-1) + 5 * 5 * 3 = 33$$

$$x = x_b a X + x_a b Y$$

Discrete Log

Modular Exponentiation

$$x \bmod N \longrightarrow x^a \bmod N$$

Discrete Log

$$y = x^a \bmod N \longrightarrow a$$

The discrete log problem is, given y and x, to find a such that $y = x^a \bmod N$. It is the inverse of modular exponentiation.

Modular exponentiation can be performed efficiently as function of the input size via repeated squaring. What about discrete log?

Repeated Squaring

We can get large exponents quickly by repeated squaring:

From $x^i \bmod N$, we can calculate $x^{2i} \bmod N$ using 1 multiplication by squaring it.

Doing this repeatedly gives us $x, x^2, x^4, x^8, \ldots, x^{2^c}$, with only c multiplications.

To calculate $x^a \bmod N$ for general a, first write a in binary:

$$a = a_0 2^c + a_1 2^{c-1} + \cdots + a_{c-1} 2 + a_c$$

Then $$x^a = \prod_{i=0}^{c} x^{a_{c-i} 2^i}$$

This needs $O(\log a)$ multiplications.

Example:

Calculate $65^{12} \bmod 71$:

$$65^2 = 36 \bmod 71$$

$$65^4 = 36^2 = 18 \bmod 71$$

$$65^8 = 18^2 = 40 \bmod 71$$

Then

$$\begin{aligned} 65^{12} &= 65^8 \cdot 65^4 \bmod 71 \\ &= 40 \cdot 18 \bmod 71 \\ &= 10 \bmod 71 \end{aligned}$$

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

Could loop through all possible a and compute $x^a \bmod N$.

This class is being recorded

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

- Could loop through all possible a and compute $x^a \bmod N$.
  - But this takes O(N) trials (or actually $O(\varphi(N))$) — not efficient in general
  - If we know $\mathrm{ord}(x)$ is small, we can do it: We only need to check powers up to $\mathrm{ord}(x)$, since we know $x^a \bmod N$ just repeats values after that.

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

Could loop through all possible a and compute $x^a \bmod N$.

But this takes O(N) trials (or actually $O(\varphi(N))$) — not efficient in general

If we know $\mathrm{ord}(x)$ is small, we can do it: We only need to check powers up to $\mathrm{ord}(x)$, since we know $x^a \bmod N$ just repeats values after that.

We could take repeated square roots to get a ballpark value for a and then narrow it down.

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

Could loop through all possible a and compute $x^a \bmod N$.

But this takes O(N) trials (or actually $O(\varphi(N))$) — not efficient in general

If we know $\mathrm{ord}(x)$ is small, we can do it: We only need to check powers up to $\mathrm{ord}(x)$, since we know $x^a \bmod N$ just repeats values after that.

We could take repeated square roots to get a ballpark value for a and then narrow it down.

This works for integers — but for mod N arithmetic, there are two problems: It is not clear how to take square roots; and taking the square root does not consistently give us something smaller in modular arithmetic unlike for integers.

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

This class is being recorded

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

We could compute powers $x^{2^i} \bmod N$ and then try to find a product of these values that gives us y.

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

We could compute powers $x^{2^i} \bmod N$ and then try to find a product of these values that gives us y.

Not easy to find which subset of possible powers of powers of 2 to multiply together to get y.

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

- We could compute powers $x^{2^i} \bmod N$ and then try to find a product of these values that gives us y.
  - Not easy to find which subset of possible powers of powers of 2 to multiply together to get y.

It appears to be hard to find the discrete log, even though computing modular exponentials is easy.

Ideas for Solving Discrete Log

How might we try to find the discrete log of y, for base x?

We could compute powers $x^{2^i} \bmod N$ and then try to find a product of these values that gives us y.

Not easy to find which subset of possible powers of powers of 2 to multiply together to get y.

It appears to be hard to find the discrete log, even though computing modular exponentials is easy.

But it is not *always* hard, for instance if the base x has low order. We should restrict attention to hard cases if we want to build a cryptographic system.

Hardness of Discrete Log

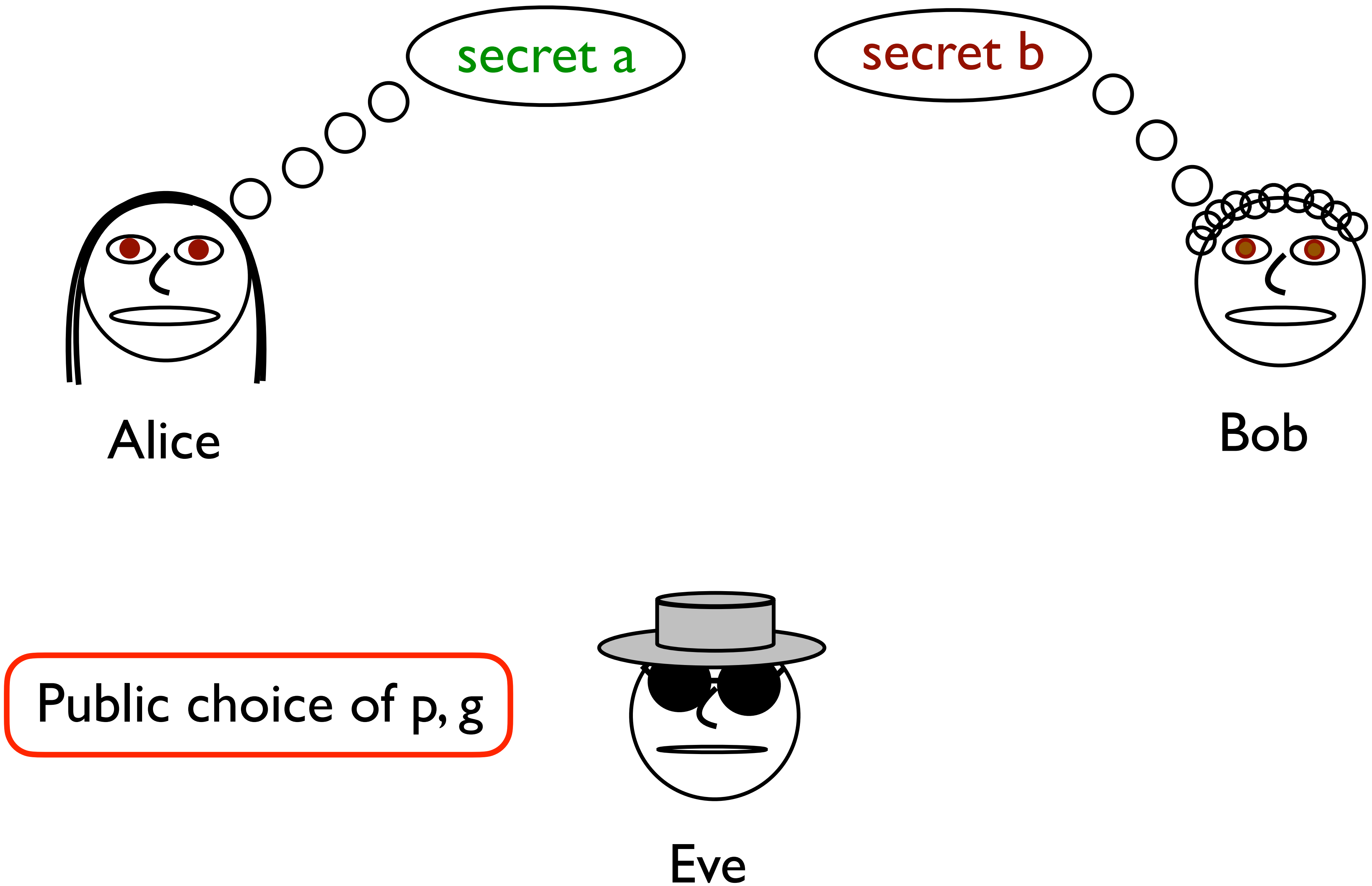
Definition: Given a security parameter s, let N_s be an s-bit long number, and let $x_s \in \mathbb{Z}^*_{N_s}$ be an element of $\mathbb{Z}^*_{N_s}$. We say that discrete log for (N_s, x_s) is worst-case hard if there is *no* polynomial time algorithm $\mathscr{A}$ such that for all $y \in \langle x_s \rangle$, $\mathscr{A}(y) = a$ with $y = x_s^a \bmod N_s$.

Recall that we are defining hardness in terms of asymptotic complexity, so we need to let the numbers get large and study how rapidly the problem gets harder in that limit.

Thus, we have a sequence of pairs (modulus, base) that get longer, and the problem is hard if it can't be solved in a time polynomial in the *length* of the numbers.

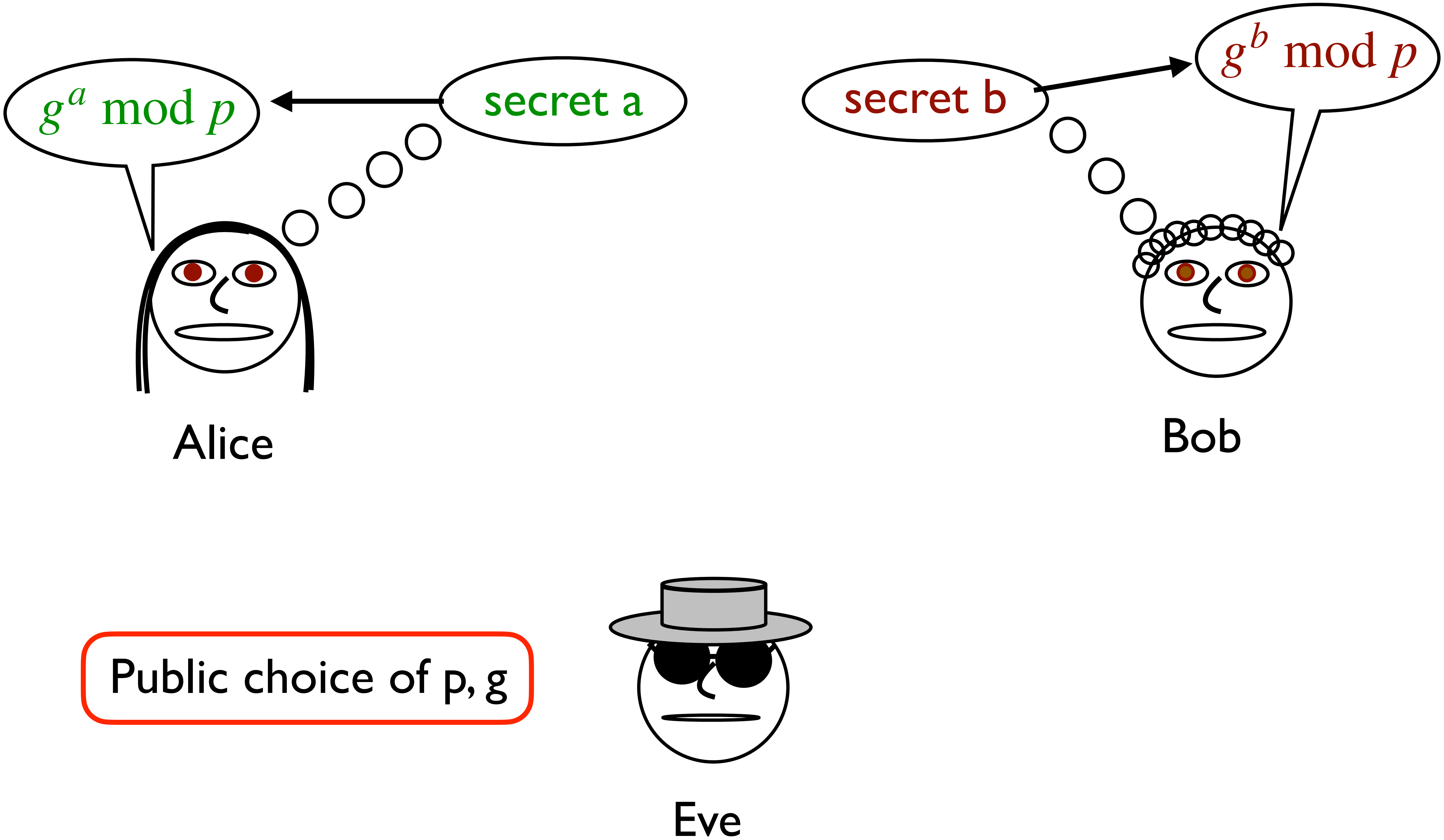
This class is being recorded

Diffie-Hellman Key Exchange



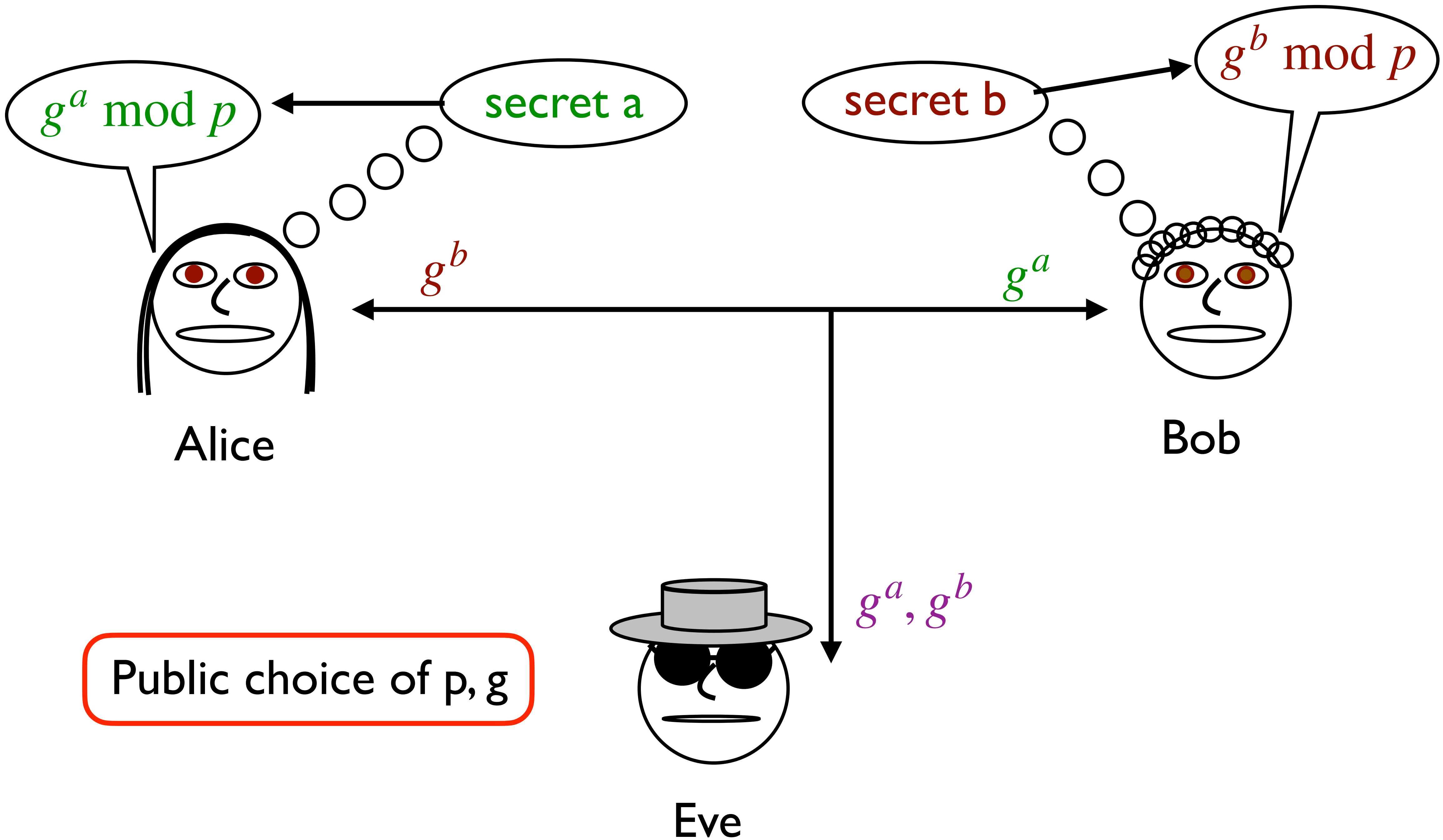
This class is being recorded

Diffie-Hellman Key Exchange



This class is being recorded

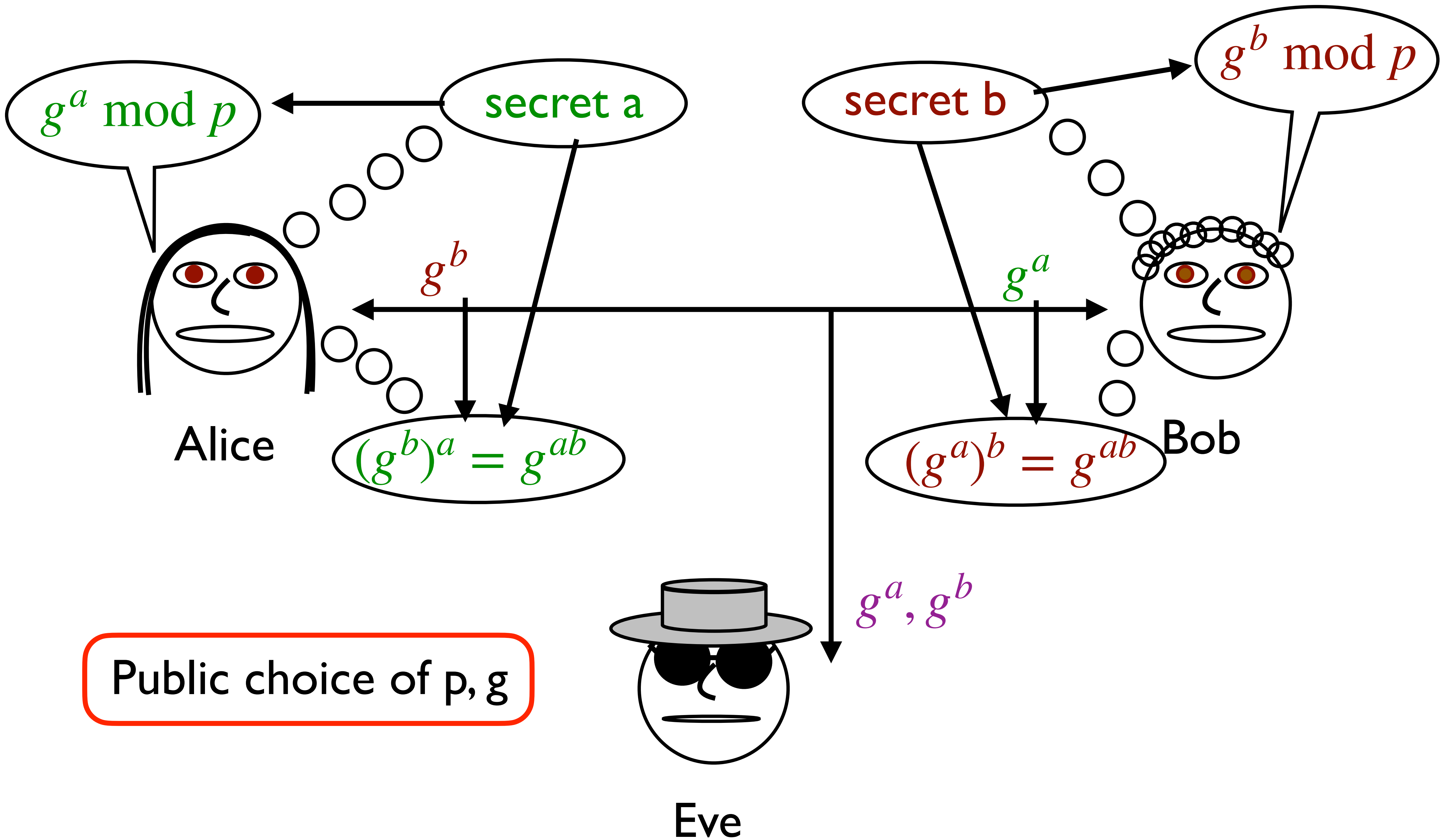
Diffie-Hellman Key Exchange



Public choice of p, g

This class is being recorded

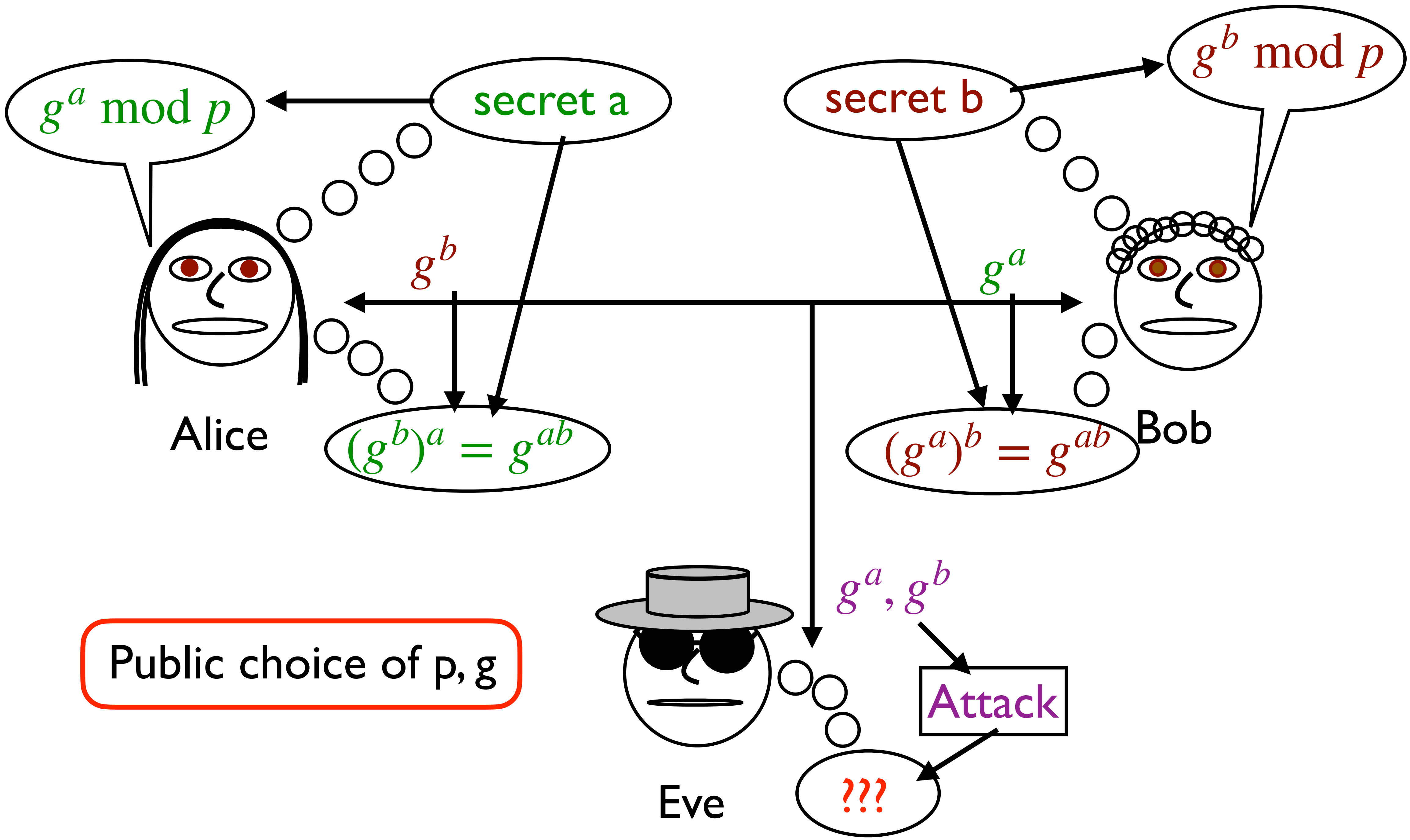
Diffie-Hellman Key Exchange



Public choice of p, g

This class is being recorded

Diffie-Hellman Key Exchange



Public choice of p, g

This class is being recorded