Lecture 19

Encryption - Part II

ECE 422: Reliable and Secure Systems Design

UNIVERSITY OF ALBERTA

Instructor: An Ran Chen
Term: 2024 Winter

Schedule for today

- Key concepts from last class
- Diffie-Hellman Key Exchange
    - Primitive roots
    - Discrete logarithm problem
- TODOs

Confidentiality

Confidentiality

- Only the authorized user can access particular resources

Methods to achieve confidentiality:

- Encryption: encoding/decoding of the plaintext
  - E.g., Symmetric/asymmetric encryption
- Access controls: restricted access
  - E.g., Our library website
- Authentication: credentials check
  - E.g., Mobile authentication for faculty and staff

UoA's Information Services & Technology

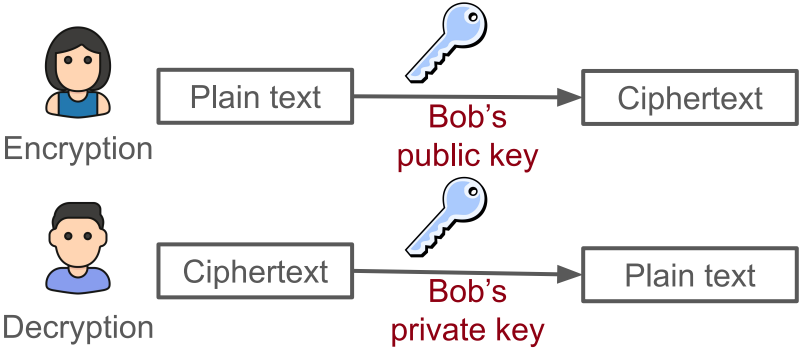
Example of asymmetric encryption

Bob generates two keys:

- public key for encryption
- private key for decryption

Alice wants to send a message to Bob

- Alice encrypts the message “hello!” with Bob’s public key.



Although the encryption key is public, it is impossible to eavesdrop:

- Bob is the only one with decryption key

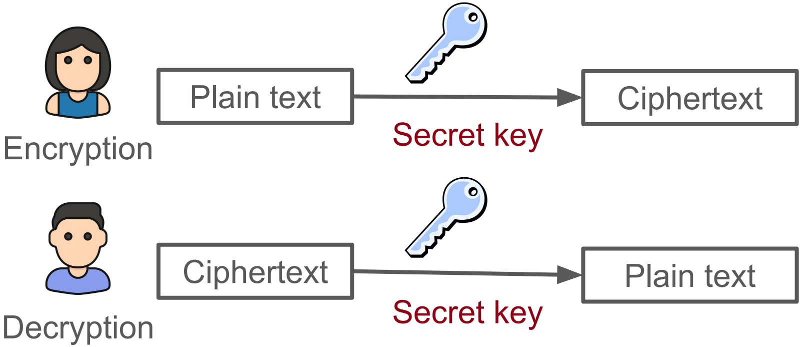
Example of symmetric encryption

Alice generates one key:

- The secret key is used for both encryption and decryption

Alice wants to send a message to Bob

- Alice shares the secret key with Bob.



With man-in-the-middle attack

- Eve can intercept the messages between Alice and Bob.
- But, worst than that, Eve can also intercept the secret key.

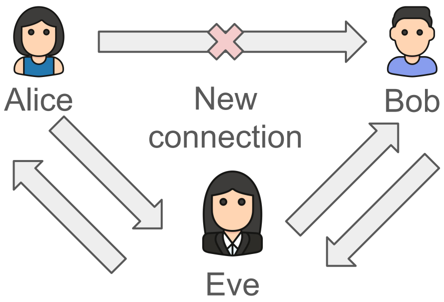
Key exchange in symmetric encryption

Contrary to asymmetric encryption, in symmetric encryption, the key exchange becomes vulnerable to man-in-the-middle attacks.

Alice wants to communicate with Bob

- Alice sends her key to Bob
- Eve can intercept the key from Alice and claim to be Bob
- At the same time, Eve can convince Bob that she is Alice

How can Alice and Bob agree on a shared secret key without letting Eve, who is always listening, also obtain the key?



Schedule for today

- Key concepts from last class
- Diffie-Hellman Key Exchange
  - Primitive roots
  - Discrete logarithm problem
- TODOs

Diffie-Hellman algorithm

Diffie-Hellman is a key exchange algorithm used with symmetric encryption.

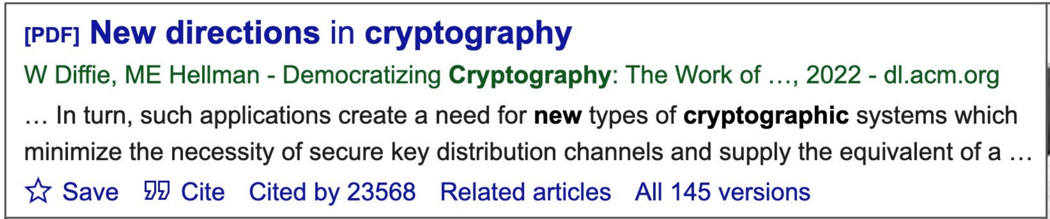
- It allows both parties to agree on an identical secret key
- Without having to share the actual key in the communication channel
- This is used for key exchange, and not encryption/decryption

Overall idea behind DF key exchange algorithm:

- Neither parties choose the key explicitly
- Both parties contribute in calculating the secret key together
- The calculated secret key can then be used in symmetric encryption.

Diffie-Hellman algorithm

Introduced by Whitfield Diffie and Martin E. Hellman (2015 Turing Award) from Stanford University in their paper: New Directions in Cryptography, 1976

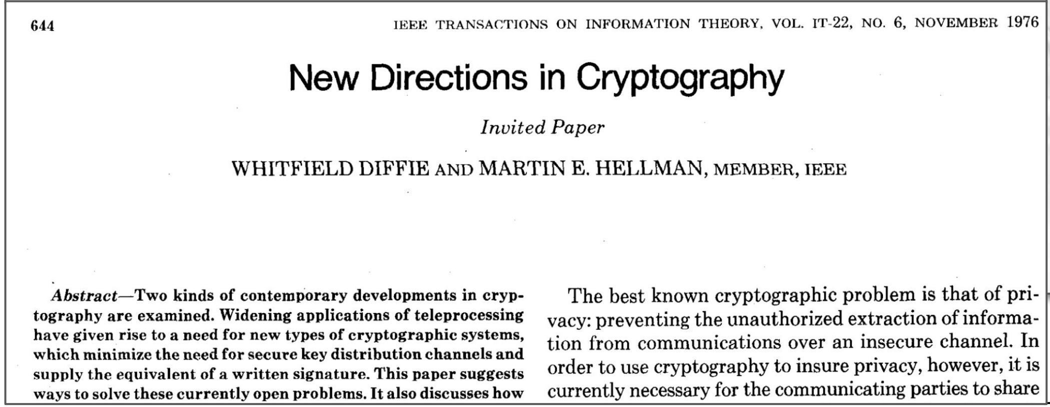


[PDF] **New directions** in **cryptography**

W Diffie, ME Hellman - Democratizing **Cryptography**: The Work of …, 2022 - dl.acm.org

… In turn, such applications create a need for **new** types of **cryptographic** systems which minimize the necessity of secure key distribution channels and supply the equivalent of a …

☆ Save ❞ Cite Cited by 23568 Related articles All 145 versions



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—**Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how**

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share

From left to right: Hellman and Diffie

Analogous to finding a shared secret color

Analogy: Alice and Bob wants to agree on a secret color without letting Eve know

Solution as a 4-steps process:

Step 1: Alice and Bob agree on a starting color

Step 2: Alice and Bob pick their secret color to come up with a mixed color

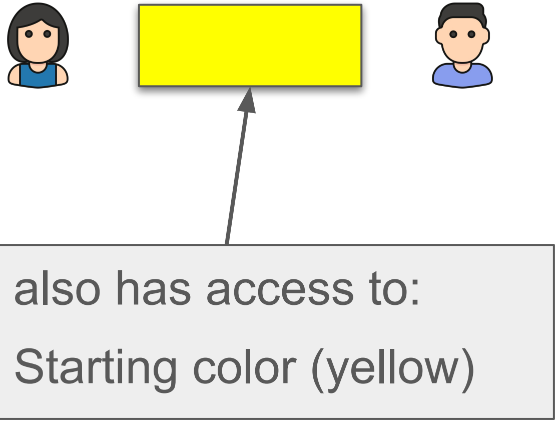
Step 3: Alice and Bob share their mixed color

Step 4: Alice and Bob get a new mixture based on each other’s mixed color and their own secret color

Analogous to finding a shared secret color

Analogy: Alice and Bob wants to agree on a secret color without letting Eve know

Step 1: Alice and Bob agree on a starting color, yellow



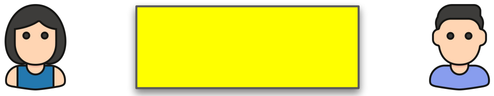
Eve also has access to:

- Starting color (yellow)

Analogous to finding a shared secret color

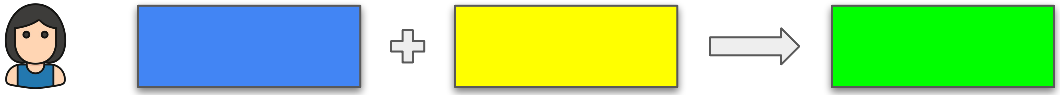
Analogy: Alice and Bob wants to agree on a secret color without letting Eve know

Step 1: Alice and Bob agree on a starting color, yellow

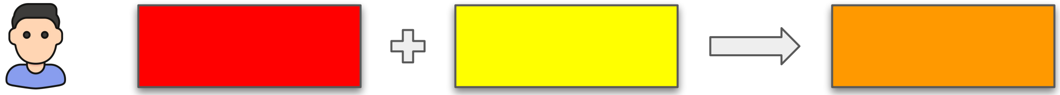


Step 2: Alice and Bob pick their secret color and mix it with the starting color

- Alice picks blue, the mixture gives green (yellow + blue)



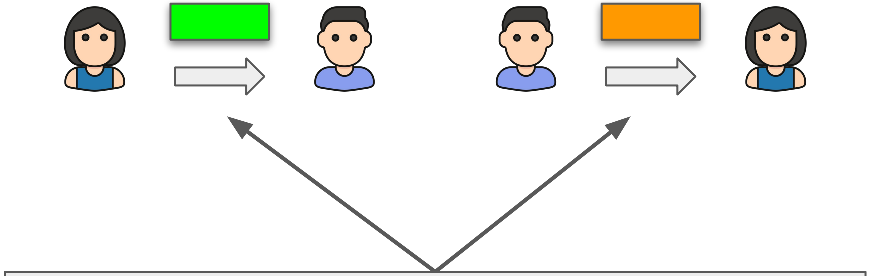
- Bob picks red, the mixture gives orange (yellow + red)



Analogous to finding a shared secret color

Analogy: Alice and Bob wants to agree on a secret color without letting Eve know

Step 3: Alice and Bob exchange the mixed color



Eve also has access to:

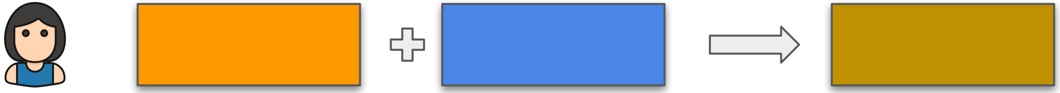
- Starting color (yellow)
- Mixed colors (green and orange)

Analogous to finding a shared secret color

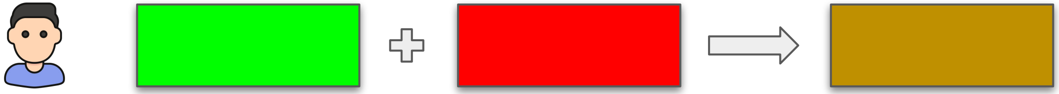
Analogy: Alice and Bob wants to agree on a secret color without letting Eve know

Step 4: Alice and Bob mix their secret color with the mixed color to get the shared secret color

- Alice mixes orange with blue, the mixture gives brown (yellow + red + blue)



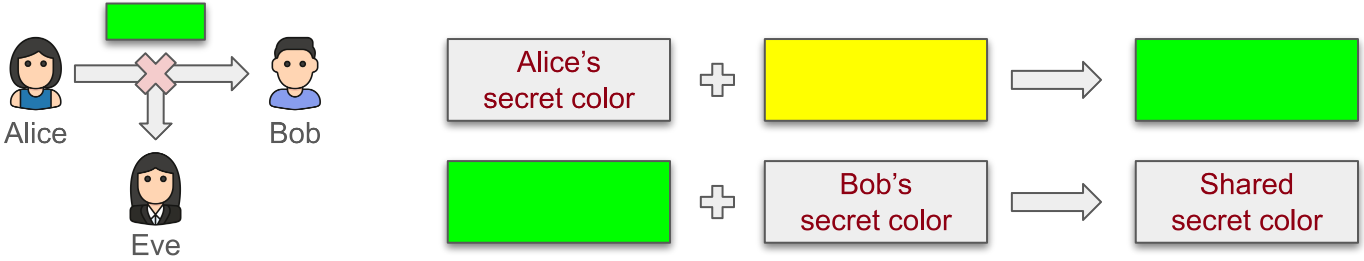
- Bob mixes green with red, the mixture gives brown (yellow + blue + red)



Analogous to finding a shared secret color

Can Eve come up with the shared secret color, brown?

- Eve has access to the starting color (yellow), and the mixed colors (green and orange), but not the secret colors (red and blue).



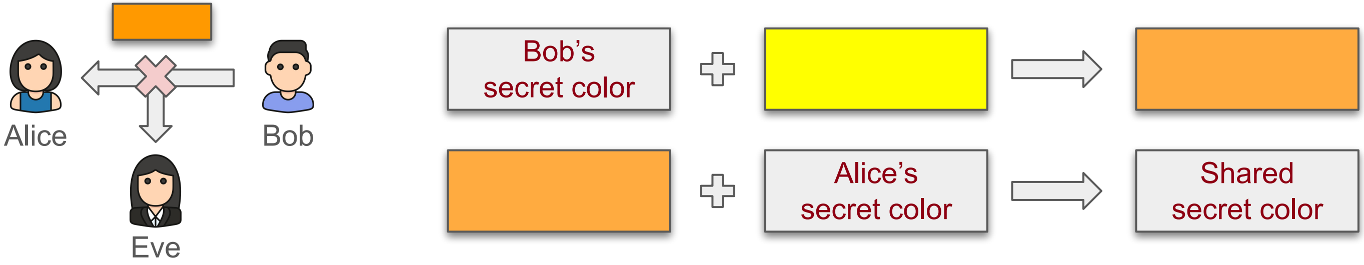
Alice

Bob

Eve

Alice's secret color + 🟨 → 🟩

🟩 + Bob's secret color → Shared secret color



Alice

Bob

Eve

Bob's secret color + 🟨 → 🟧

🟧 + Alice's secret color → Shared secret color

DF algorithm

DF algorithm as a 4-steps process:

Step 1: Alice and Bob agree on some public parameters (starting color)

Step 2: Alice and Bob pick their secret integer (secret color) to come up with a public integer (mixed color)

Step 3: Alice and Bob exchange their own public integer (mixed color)

Step 4: Alice and Bob compute the shared secret key based on the exchanged public integer (mixed color) and their own secret integer (secret color)

DF algorithm

Step 1: Alice and Bob agree on some public parameters

- a (large) prime number *p*
- an integer *g*

The integer *g* must be a primitive root to the prime number *p*.

Example

- p = 17
- g = 3

Primitive roots

An integer *g* is a primitive root mod p if every integer *a* coprime to p is congruent to a power of *g* mod *p*.

- Example: 2 is a primitive root mod 5, because for every number *a* that is coprime to 5 (e.g., 1, 2, 3, 4), there is an integer z such that $2^z \bmod (5) = a$.

For g to be a primitive root mod p, there are two conditions:

- $1 < g < p$
- The following modular results must be distinct:
    - g^1 mod p
    - g^2 mod p
    - …
    - g^{p-1} mod p

Primitive roots

Example: To verify that 2 is a primitive root of prime number 5:

- For every integer coprime to 5, there must be a power of 2 that is congruent

- Integers that are coprimes to 5: 1, 2, 3, 4
- z = 1, 2^1 mod(5) = 2
- z = 2, 2^2 mod(5) = 4
- z = 3, 2^3 mod(5) = 3
- z = 4, 2^4 mod(5) = 1
- Verified: For 1, 2, 3, 4, there is a power of 2 that is congruent

Primitive roots

Question: Is 3 a primitive root of prime number 7?

Primitive roots

Question: Is 3 a primitive root of prime number 7?

Answer: Yes, 3 is a primitive root of 7.

- For every integer coprime to 7, there is a power of 3 that is congruent.
- Integers that are coprimes to 7: 1, 2, 3, 4, 5, 6
- 3^1 mod(7) = 3
- 3^2 mod(7) = 2
- 3^3 mod(7) = 6
- 3^4 mod(7) = 4
- 3^5 mod(7) = 5
- 3^6 mod(7) = 1
- Verified: For 1, 2, 3, 4, 5, 6, there is a power of 3 that is congruent

DF algorithm

Step 1: Alice and Bob agree on some public parameters

- a (large) prime number *p*
- an integer *g*

The integer *g* must be a primitive root to the prime number *p*.

Example

- p = 17
- g = 3

DF algorithm

Step 2: Alice and Bob pick their secret integer to come up with a public integer

Alice’s private computation

- Select a secret integer a, $a < p$
- Compute the public integer A = $g^a \mathit{mod}(p)$

Example

Alice’s private computation

- a = 15, 15 < 17
- $A = 3^{15}$ mod (17) = 6

The public integer *A* will be shared, but the integer *a* remains secret.

DF algorithm

Step 2: Alice and Bob pick their secret integer to come up with a public integer

Alice's private computation

- Select a secret integer a, $a < p$
- Compute the public integer A = $g^a \; mod(p)$

Bob's private computation

- Select a random number b, $b < p$
- Compute the public integer B = $g^b \; mod(p)$

Example

Alice's private computation

- a = 15, 15 < 17
- $A = 3^{15}$ mod (17) = 6

Bob's private computation

- b = 13, 13 < 17
- $B = 3^{13}$ mod (17) = 12

DF algorithm

Step 3: Alice and Bob exchange their own public integer

Bob sends B to Alice. Alice has access to

- a, her secret integer
- B, Bob's public integer

Example

Alice has:

- $a = 15$, $A = 6$
- B = 12

DF algorithm

Step 3: Alice and Bob exchange their own public integer

Bob sends B to Alice. Alice has access to

- *a*, her secret integer
- *B*, Bob's public integer

Alice sends A to Bob. Bob has access to:

- *b*, his secret integer
- *A*, Alice's public integer

Example

Alice has:

- $a = 15$, $A = 6$
- B = 12

Bob's private computation

- b = 13, B = 12
- $A = 6$

DF algorithm

Step 4: Alice and Bob compute the shared secret key

Alice's private computation

- Compute the shared secret key $K = B^a \bmod(p)$

Shared secret key

- $K = g^{ab} \bmod(p)$

Bob's public integer B

- $B = g^b \bmod(p)$

Therefore:

- $K = (g^b)^a \bmod(p) = B^a \bmod (p)$

Example

Alice computes:

- $K = 12^{15} \bmod (17) = 10$

DF algorithm

Step 4: Alice and Bob compute the shared secret key

Alice's private computation

- Compute the shared secret key
  $K = B^a \ mod(p)$

Bob's private computation

- Compute the shared secret key
  $K = A^b \ mod(p)$

Example

Alice computes:

- $K = 12^{15} \text{ mod } (17) = 10$

Bob computes:

- $K = 6^{13} \text{ mod } (17) = 10$

DF algorithm cheat sheet

DF algorithm as a 4-steps process:

Step 1: Alice and Bob agree on some public parameters

Step 2: Alice and Bob come up with a public integer

Step 3: Alice and Bob exchange their own public integer

Step 4: Alice and Bob compute the shared secret key

Public integers

- $A = g^a \mod(p)$
- $B = g^b \mod(p)$

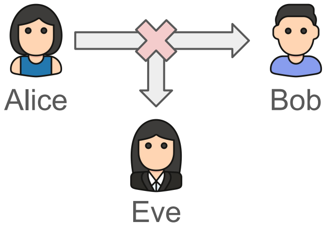
Shared secret key

- $K = g^{ab} \mod(p) = A^b \mod(p)$
- $K = g^{ba} \mod(p) = B^a \mod(p)$

DF algorithm

Can Eve come up with the shared secret key?

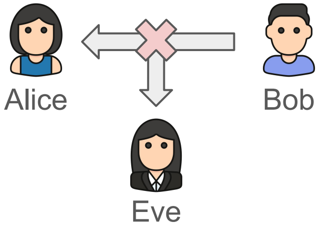
- Eve has access to the public parameters (p, g), and the public integers (A, B), but not the secret integers (a and b), which are required to find the secret key.



$$A = g^{a} \mod(p)$$

$$A = g^{?} \mod(p)$$

→ A Discrete Logarithm Problem (DLP)



$$B = g^{b} \mod(p)$$

$$B = g^{?} \mod(p)$$

→ A Discrete Logarithm Problem (DLP)

Discrete Logarithm Problem (DLP)

A discrete log problem is defined as:

Given $g^a\ mod(p) = b,\ solve\ for\ a$
where *a* is a primitive root and *p* is a prime number.

Solving a discrete log problem is hard, because of the primitive root property

- Given any exponent, the solution to $g^a\ mod(p)$ is uniformly distributed
- Each solution is equally likely to happen

DF algorithm

Step 1: Alice and Bob agree on some public parameters

- a (large) prime number *p*
- an integer *g*

The integer *g* must be a primitive root to the prime number *p*.

Example

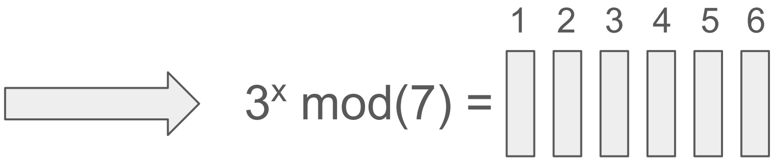
- p = 17
- g = 3

Primitive roots

Example: To verify that 3 is a primitive root of prime number 7:

- Coprimes of 7: 1, 2, 3, 4, 5, 6
- 3^1 mod(7) = 3
- 3^2 mod(7) = 2
- 3^3 mod(7) = 6
- 3^4 mod(7) = 4
- 3^5 mod(7) = 5
- 3^6 mod(7) = 1

- 3^7 mod(7) = 3
- 3^8 mod(7) = 2
- 3^9 mod(7) = 6
- 3^{10} mod(7) = 4
- 3^{11} mod(7) = 5
- 3^{12} mod(7) = 1

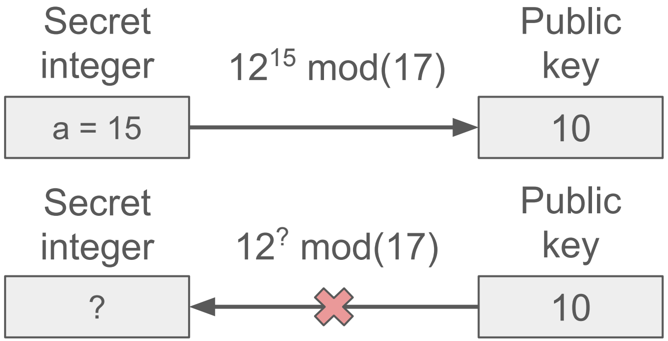


Property of a primitive root: when raised to an exponent, the solution is distributed uniformly.

Discrete Logarithm Problem (DLP)

For Eve to find the secret integer, she needs to solve the discrete logarithm problem, however

- It is easy to calculate the public key
- Hard to find the secret integer (many solutions)



The idea is similar to the shared secret color solution:

- Easy to mix a secret color with the starting one to get a mixture
- Hard to find the secret color from the mixed color (many color combinations)

Question on DF algorithm

Suppose that Alice and Bob agree on g = 2 and p = 19.

Question: What is the secret key if Alice chooses 6 and Bob chooses 8 as their respective secret integers? (show the calculations for both Alice and Bob)

Public integers

- $A = g^a \mod(p)$
- $B = g^b \mod(p)$

Shared secret key

- $K = g^{ab} \mod(p) = A^b \mod(p)$
- $K = g^{ba} \mod(p) = B^a \mod(p)$

Question on DF algorithm

Suppose that Alice and Bob agree on g = 2 and p = 19.

Question: What is the secret key if Alice chooses 6 and Bob chooses 8 as their respective secret integers? (show the calculations for both Alice and Bob)

Intuition: Given the value of g, p, a and b, calculate K

Public integers

- $A = g^a \, mod(p)$
- $B = g^b \, mod(p)$

Shared secret key

- $K = g^{ab} \, mod(p) = A^b \, mod(p)$
- $K = g^{ba} \, mod(p) = B^a \, mod(p)$

Question on DF algorithm

Suppose that Alice and Bob agree on g = 2 and p = 19.

Question: What is the secret key if Alice chooses 6 and Bob chooses 8 as their respective secret integers? (show the calculations for both Alice and Bob)

Answer: Calculate the public integers A and B to find out K.

For Alice:

- $A = g^a \; mod(p) = 2^6 \bmod (19) = 7$
- $K = B^a \; mod(p) = 9^6 \bmod (19) = 11$

For Bob:

- $B = g^b \; mod(p) = 2^8 \bmod (19) = 9$
- $K = A^b \; mod(p) = 7^8 \bmod (19) = 11$

Public integers

- $A = g^a \; mod(p)$
- $B = g^b \; mod(p)$

Shared secret key

- $K = g^{ab} \; mod(p) = A^b \; mod(p)$
- $K = g^{ba} \; mod(p) = B^a \; mod(p)$

TODOs

- Project 2 Hints and FAQs are posted under Week 6
  - Make sure to check it out, send your questions on Slack
- No class on Monday, March 4
  - Students' Union Election Forum