Announcements

- Homework 14 (LAST ONE!!!) due on Monday, April 25th at 11:59pm
  - If you want me to open up any old homeworks, email me!!
  - If you do a problem which has to be hand graded, let me know when you finish it.
- Exam 3 on Thursday, April 28th from 12:00-2:30pm
  - Both in person (here), and/or virtually
  - ONLY covers cryptography
- Final grade calculation:

  15% Lowest Exam + 20% Middle Exam + 30% Highest Exam + 35% Homework*

  *After dropping lowest two homework grades

Diffie-Hellman and Public Key Cryptography

4/19/22

Example

In a Diffie-Hellman Key Exchange, some of the numbers involved are a generator g, a large prime p, exponents a and b, exchanged values $M = g^a$ and $N = g^b$, and the value $M^b = N^a$.

Which of these numbers are *public* (i.e. it's okay if an eavesdropper Eva sees them)?

(A) Only g and p

(B) Only g, p, M, and N

(C) Only g, p, M, N, and $M^b = N^a$

(D) Only g, p, M, N, a, and b

Example

In a Diffie-Hellman Key Exchange, some of the numbers involved are a generator g, a large prime p, exponents a and b, exchanged values $M = g^a$ and $N = g^b$, and the value $M^b = N^a$.

If Ari and Bo are the ones doing the exchange (Ari's exponent is a and Bo's exponent is b), which of the numbers will Ari know by the end of the exchange?

(A) Only g, p, M, and N

(B) Only g, p, a, and M

(C) Only g, p, a, M, and $M^b = N^a$

(D) Only g, p, a, M, N, and $M^b = N^a$

(E) Ari will know all of g, p, M, N, a, b, and $M^b = N^a$

Choosing the prime p

The prime p should be big enough that in arithmetic mod p, discrete logarithms are expensive, but small enough that modular exponentiation is cheap.

Public Key Cryptography

- Diffie-Hellman Key Exchange lets parties who wish to communicate securely create a shared secret key (to be used in some cryptosystem)

Public Key Cryptography

- Diffie-Hellman Key Exchange lets parties who wish to communicate securely create a shared secret key (to be used in some cryptosystem) $\longrightarrow$ Solved the key distribution problem!

Public Key Cryptography

- Diffie-Hellman Key Exchange lets parties who wish to communicate securely create a shared secret key (to be used in some cryptosystem) $\longrightarrow$ Solved the key distribution problem!
- DH and variations are still used today

Public Key Cryptography

- Diffie-Hellman Key Exchange lets parties who wish to communicate securely create a shared secret key (to be used in some cryptosystem) $\longrightarrow$ Solved the key distribution problem!
- DH and variations are still used today
- Other widely used public key cryptosystem: RSA

Public Key Cryptography

- Today, most digital secure communication relies on DH and RSA

Public Key Cryptography

- Today, most digital secure communication relies on DH and RSA

- **Implication:** If someone finds a shortcut for discrete logarithms (DH) or factoring (RSA), these cryptosystems will no longer be secure.

Public Key Cryptography

- Today, most digital secure communication relies on DH and RSA

- **Implication:** If someone finds a shortcut for discrete logarithms (DH) or factoring (RSA), these cryptosystems will no longer be secure.

- In 1994, Peter Shor discovered algorithm is a shortcut for factoring large numbers (but it relies on quantum computers, which are still being developed)

Public Key Cryptography

- Today, most digital secure communication relies on DH and RSA
- **Implication:** If someone finds a shortcut for discrete logarithms (DH) or factoring (RSA), these cryptosystems will no longer be secure.
- In 1994, Peter Shor discovered algorithm is a shortcut for factoring large numbers (but it relies on quantum computers, which are still being developed)
- Quantum cryptography???

Public Key Cryptography

- Today, most digital secure communication relies on DH and RSA
- **Implication:** If someone finds a shortcut for discrete logarithms (DH) or factoring (RSA), these cryptosystems will no longer be secure.
- In 1994, Peter Shor discovered algorithm is a shortcut for factoring large numbers (but it relies on quantum computers, which are still being developed)
- Quantum cryptography???
- "The Code Book" - Simon Singh

Homework 14 - Problem 2

You are doing a Diffie-Hellman-Merkle key exchange with Dylan using generator 2 and prime 29. You pick the secret number 14. What value will you send to Dylan?

Homework 14 - Problem 3

You are doing a Diffie-Hellman-Merkle key exchange with Juan using generator 3 and prime 17. Your secret number is 15. Juan sends you the value 2. Determine the shared secret key.

Homework 14 - Problem 4

Find the discrete logarithm base 5 of 12 mod 17. That is, what power of 5 is congruent to 12 mod 17? (Your answer must be a number between 1 and 17.)

Homework 14 - Problem 5

Mikayla and John are doing a Diffie-Hellman-Merkle key exchange using generator 3 and prime 17. You are an eavesdropper trying to figure out their private keys and the shared secret. Since you don't know the private keys, you'll need to use brute force to figure them out.

Mikayla sends John the value 13, and John sends Mikayla the value 15.

- Mikayla's Secret key:
- John's Secret key:
- Shared Secret key:

Homework 14 - Problem 6

In this problem, you will quickly calculate $2^{37} \mod 83$ (without actually needing to do 37 multiplication steps).

Take advantage of repeated squaring to find the following. Remember that $b^{2k} = (b^k)^2$, so to get from one result to the next, you can just square the previous result (and reduce mod 83 of course).

- $2^2 \mod 83 \equiv$
- $2^4 \mod 83 \equiv$
- $2^8 \mod 83 \equiv$
- $2^{16} \mod 83 \equiv$
- $2^{32} \mod 83 \equiv$
- $2^{37} \mod 83 \equiv$

Exam 3

Book Chapter on Cryptography (not every topic from the textbook was covered)

- Terminology from cryptography (cryptosystem, key, plaintext, ciphertext, encryption, decryption, sender, intended recipient, eavesdropper)
- Caesar shift cipher (encrypt and decrypt)
- General substitution cipher (encrypt and decrypt)
- Vigenère cipher (encrypt and decrypt)
    - One-time pad
- Breaking Caesar shift or general substitution using frequency analysis
- Modular arithmetic (addition, subtraction, multiplication, exponentiation, discrete logarithms)
- Diffie-Hellman (using the protocol, why it is hard for an eavesdropper to find the shared secret, what problem does it solve, how is it different from a cryptosystem)