ROYAL UNIVERSITY
OF PHNOM PENH

Introduction to Cryptography

IC: Practical Aspects of Modern Cryptography

12 Feb 2022 by Lecturer: Chap Chanpiseth

Outline

1) Cryptography
2) Cryptography for Computer Security Concepts
3) Types of cryptography
4) Novel Applications of Cryptography in Digital Communications
5) Applied Cryptography For CyberSecurity
6) A quick overview of two cryptographic techniques
    i. Remote Coin Flipping
    ii. Diffie-Hellman Key Exchange

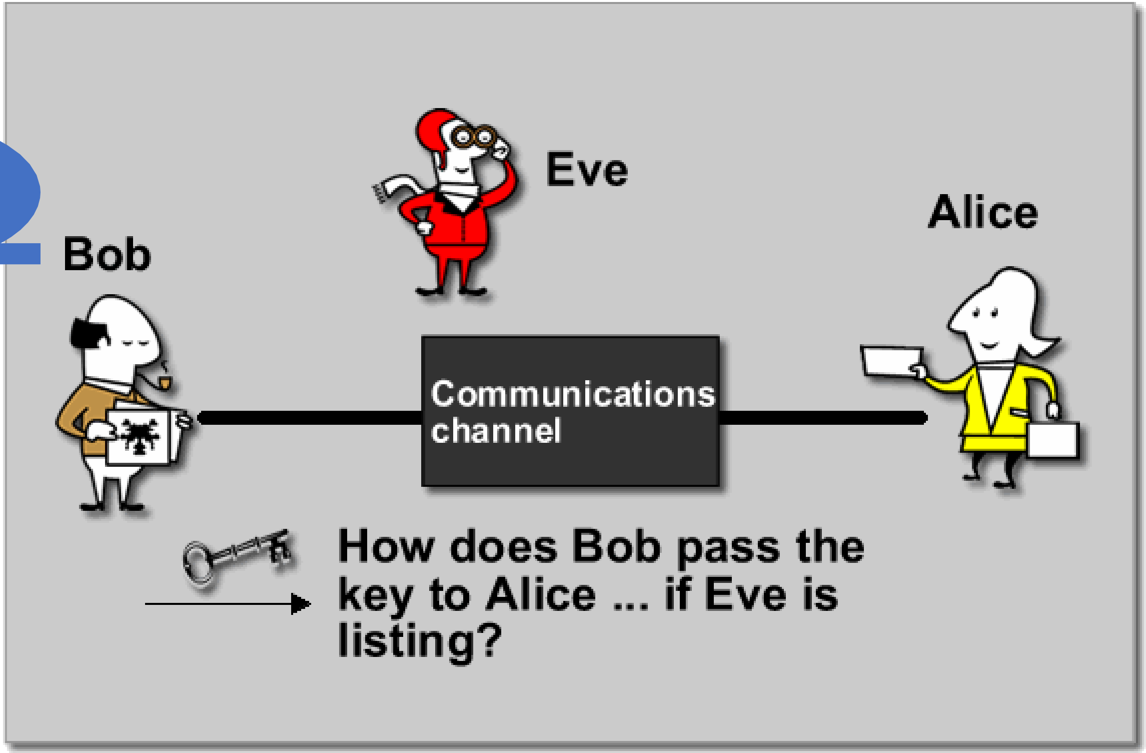
Cryptography is…

- Protecting Privacy of Data
- Authentication of Identities
- Preservation of Integrity

Basically, any protocols designed to operate in an environment *absent* of universal trust.

Alice, Bob, and Eve - Cryptography and Information Theory

Alice talking to Bob

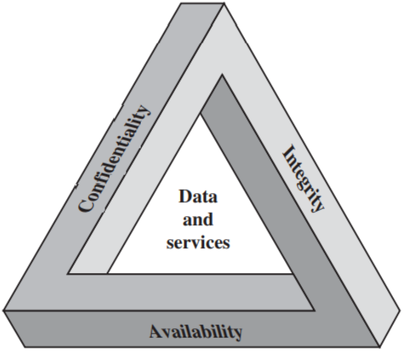


Cryptography in Computer Security Concepts

- Three key objectives that are at the heart of computer security known as **CIA triad.**

1) **Confidentiality:**

   - **Data confidentiality:** Assures that private or confidential information is not made
- available or disclosed to unauthorized individuals.
   - **Privacy:** Assures that individuals' control or influence what information related to them may be collected
- and stored and by whom and to whom that information may be disclosed.



2) **Integrity:**

   - **Data integrity:** Assures that information and programs are changed only if a specified and authorized manner.
   - **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

3) **Availability:** Assures that systems work promptly and service is not denied to authorized users.

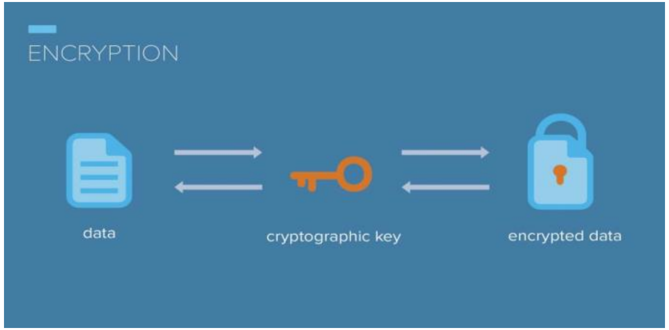
Cryptography in Computer Security Concepts (Cont.)

- The definition of CIA

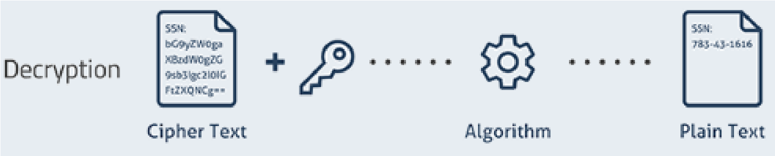
1) **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
2) **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
3) **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Definition of Encryption & Decryption

- **Encryption** is a process in which a plain text is transformed into a ciphertext by the use of a key. Decryption is the reverse of process.



- **Decryption** is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.



Definition of Encryption, Decryption

There are several ways of classifying cryptographic algorithms. they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use.

1) **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for ***privacy and confidentiality.***
2) **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption; also called asymmetric encryption. ***Primarily used for authentication, non-repudiation, and key exchange***.
3) **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. ***Primarily used for message integrity.***

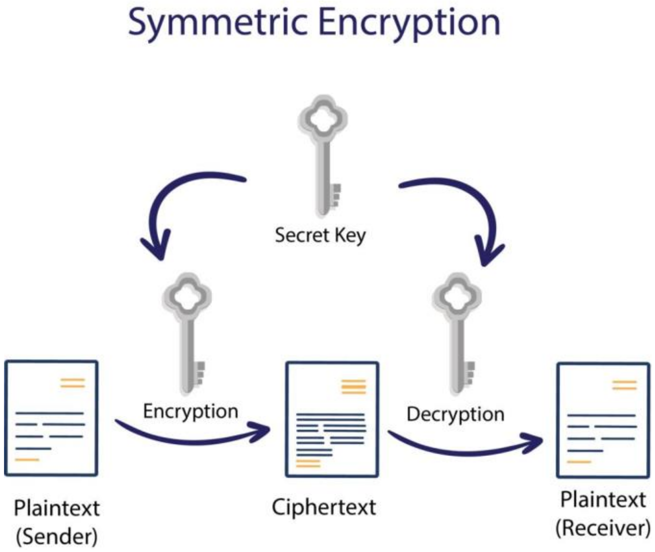
Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use.

1) **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for ***privacy and confidentiality.***
2) **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption; also called asymmetric encryption. ***Primarily used for authentication, non-repudiation, and key exchange***.
3) **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. ***Primarily used for message integrity.***

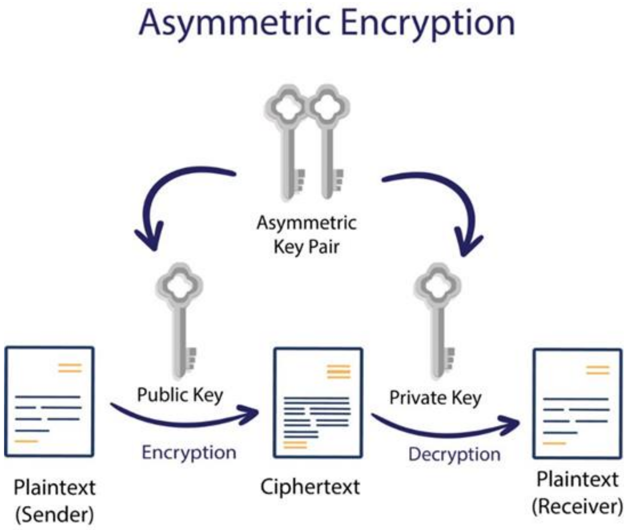
Types of Cryptographic Algorithms: Secret Key Cryptography (SKC)

1) **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for ***privacy and confidentiality***.



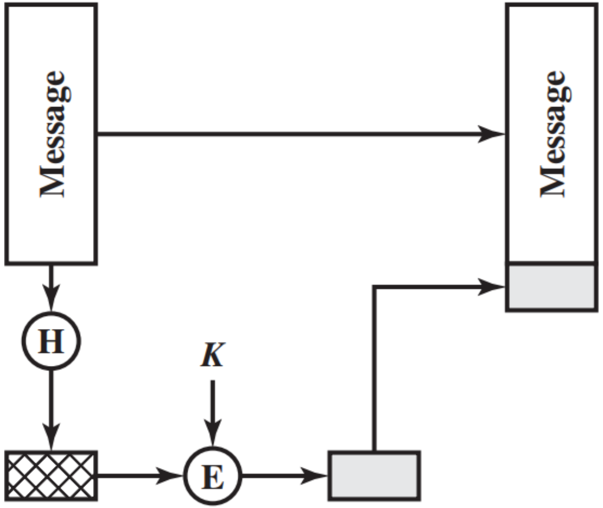
Types of Cryptographic Algorithms: Public Key Cryptography (PKC)

2) **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption; also called asymmetric encryption. ***Primarily used for authentication, non-repudiation, and key exchange.***



Types of Cryptographic Algorithms: Hash Functions

3) **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. ***Primarily used for message integrity.***



```
Hash string 1: The quick brown fox jumps over the lazy dog
Hash string 2: The quick brown fox jumps over the lazy dog.

MD5 [hash string 1] = 37c4b87edffc5d198ff5a185cee7ee09
MD5 [hash string 2] = 0d7006cd055e94cf614587e1d2ae0c8e

SHA1 [hash string 1] = be417768b5c3c5c1d9bcb2e7c119196dd76b5570
SHA1 [hash string 2] = 9c04cd6372077e9b11f70ca111c9807dc7137e4b
```

Novel Applications of Cryptography in Digital Communications

Novel Applications of Cryptography in Digital Communications

- **Electronic Mail and Data Interchange**
    - INTERNET has adopted public-key techniques for both key management for conventional encryption devices and for creating digital signatures for messages.
    - These electronic signatures are also being considered for Electronic Data Interchange (EDI), where contracts and purchase orders can be signed and delivered electronically.
    - The non-repudiation property of these digital signatures is what can make EDI work securely and force the timely controls needed in "just-in-time" manufacturing.
- **Access Control**
    - Identification of individuals is one of the basic requirements of access control, whether it is for access into buildings, into authorization of credit at a point of sale, or into computers and communication networks.
    - Typically, authentication of an individual can be based on what a person has, what a person knows, and what a person is as measured by biometrics.

Novel Applications of Cryptography in Digital Communications

- **Audit Trails**
  - Computer crimes are primarily due to authorized users of a system.
  - Computer network users are initially tempted to defraud a system when they observe that certain entry errors are undetected.
  - One way to inhibit such fraud is to trace errors to Individual users. With a smart card, each access time and terminal location can be recorded onto the smart card by the terminal.

Novel Applications of Cryptography in Digital Communications

- **Software Verification & Virus Detection**
  - A software package can be thought of as a message which can be signed by the producer of the software. With public-key signatures anyone can verify the authenticity of the signature and the integrity of the software package.
  - Although this does not protect against copies, this use of public signatures can be used to verify that the software has not been altered since the manufacturer signed it. Game machines, for example, can be designed to run only authorized game programs with the appropriate signatures.
  - This software verification scheme assumes that there is a trusted and protected module that does the verification of signatures, and that this unit cannot be bypassed.

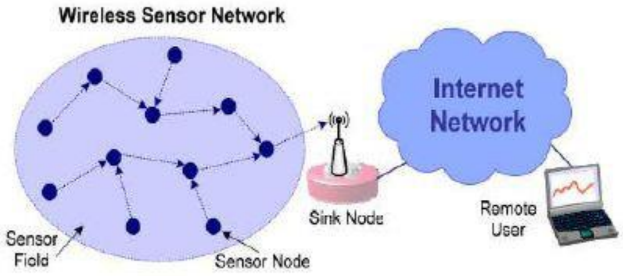
Applied Cryptography For CyberSecurity

Definition of Cybersecurity

- In simple words, Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

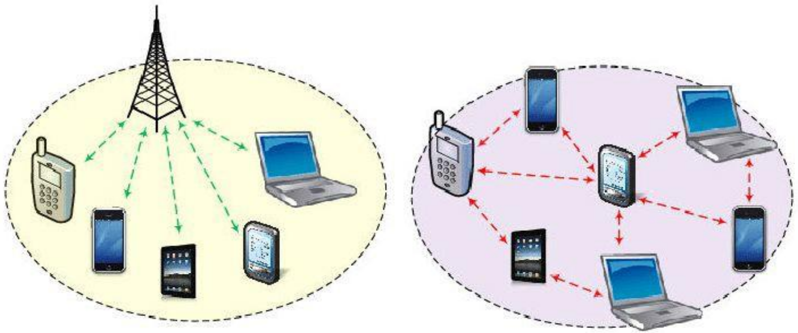
Cryptography in Wireless Communication

- **Applied Cryptography in Wireless Sensor Networks**
  - A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.
  - A collection of sensing devices that can communicate wirelessly.



Applied Cryptography in Infrastructure-Free Wireless Networks

- **Applied Cryptography in Infrastructure-Free Wireless Networks**
  - Wireless networks can be generally categorized into 2 type according to their communication mechanisms.
    1. Infrastructure-based
    2. Infrastructure-less



Infrastructure-based wireless networks

Wireless ad hoc networks

A quick overview of three cryptographic techniques

Remote Coin Flipping

- Alice and Bob decide to make a decision by flipping a coin.
- Alice and Bob are not in the same place.

Remote Coin Flipping

- Alice and Bob decide to make a decision by flipping a coin.
- Alice and Bob are not in the same place.

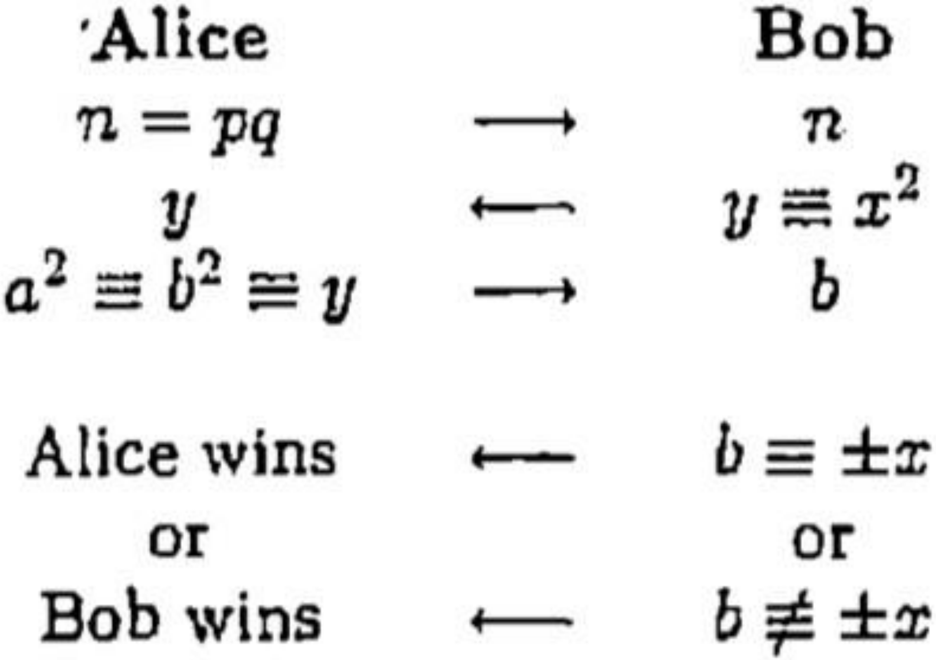
Ground Rule

- We cannot assume simultaneous actions.
- Players must take turns.

Two-part answer:

- NO – I will sketch a formal proof.
- YES – I will provide an effective protocol.

Is Remote Coin Flipping Possible?



Alice		Bob
$n = pq$	$\longrightarrow$	n
y	$\longleftarrow$	$y \equiv x^2$
$a^2 \equiv b^2 \equiv y$	$\longrightarrow$	b
Alice wins	$\longleftarrow$	$b \equiv \pm x$
or		or
Bob wins	$\longleftarrow$	$b \not\equiv \pm x$

- Two large random primes p and q, both congruent to 3 mod 4
-

=> If b = ±x (mod n), Bob tells Alice that she wins.

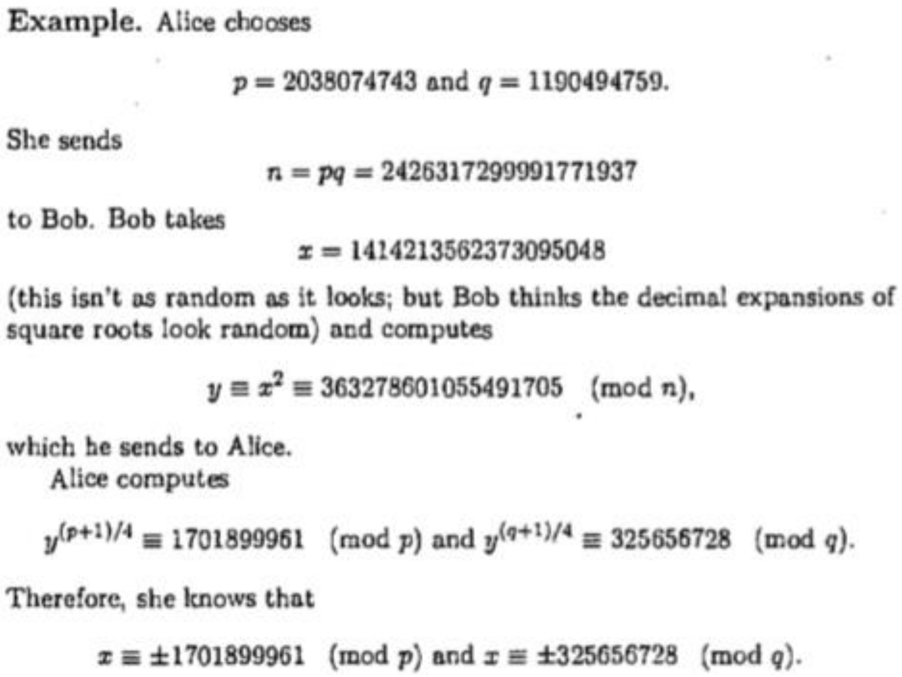
=> If b # ±x (mod n), Bob wins.

Chinese Remaindering

- If $N = PQ$, then a computation mod N can be accomplished by performing the same computation mod P and again mod Q and then using Chinese Remaindering to derive the answer to the mod N computation.

- If $X = A \bmod P$ and $X = B \bmod Q$ then
  as long as P and Q have no common factors, X can be derived as
  - $X = A \cdot Q \cdot (Q^{-1} \bmod P) + B \cdot P \cdot (P^{-1} \bmod Q)$.

Definition: Frequent Itemset



Example. Alice chooses

$$p = 2038074743 \text{ and } q = 1190494759.$$

She sends

$$n = pq = 2426317299991771937$$

to Bob. Bob takes

$$x = 1414213562373095048$$

(this isn't as random as it looks; but Bob thinks the decimal expansions of square roots look random) and computes

$$y \equiv x^2 \equiv 363278601055491705 \pmod{n},$$

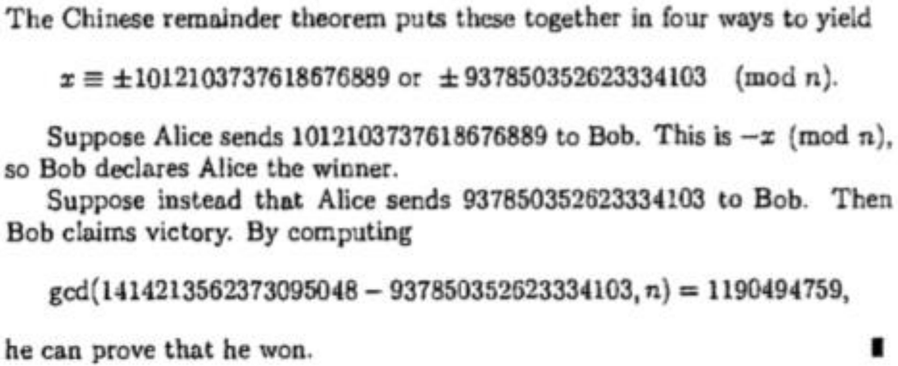
which he sends to Alice.

Alice computes

$$y^{(p+1)/4} \equiv 1701899961 \pmod{p} \text{ and } y^{(q+1)/4} \equiv 325656728 \pmod{q}.$$

Therefore, she knows that

$$x \equiv \pm 1701899961 \pmod{p} \text{ and } x \equiv \pm 325656728 \pmod{q}.$$



The Chinese remainder theorem puts these together in four ways to yield

$$x \equiv \pm 1012103737618676889 \text{ or } \pm 937850352623334103 \pmod{n}.$$

Suppose Alice sends 1012103737618676889 to Bob. This is $-x \pmod{n}$, so Bob declares Alice the winner.

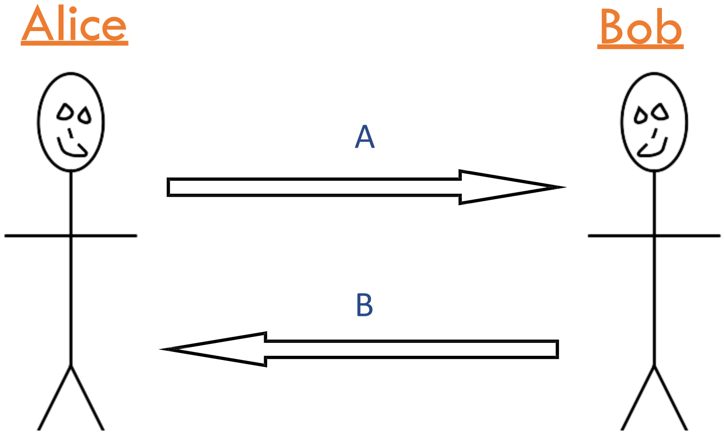
Suppose instead that Alice sends 937850352623334103 to Bob. Then Bob claims victory. By computing

$$\gcd(1414213562373095048 - 937850352623334103, n) = 1190494759,$$

he can prove that he won. ∎

Diffie-Hellman Key Exchange

The **Diffie–Hellman key exchange method** allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.



Diffie-Hellman Key Exchange

Alice

- Randomly select a large integer a and send

  A $= Y^a \bmod N$.

Bob

- Randomly select a large integer b and send

  B $= Y^b \bmod N$.

Diffie-Hellman Key Exchange

Alice

- Randomly select a large integer a and send
  $A = Y^a \bmod N$
- Compute the key
  $K = B^a \bmod N$

Bob

- Randomly select a large integer b and send
  $B = Y^b \bmod N$
- Compute the key
  $K = A^b \bmod N$

Diffie-Hellman Key Exchange

Alice

- Randomly select a large integer a and send
  $A = Y^a \bmod N$
- Compute the key
  $K = B^a \bmod N$

Bob

- Randomly select a large integer b and send
  $B = Y^b \bmod N$
- Compute the key
  $K = A^b \bmod N$

$$B^a = Y^{ba} = Y^{ab} = A^b$$

Diffie-Hellman Key Exchange

What does Eve see?

Y, Y^a, Y^b

… but the exchanged key is Y^{ab}.

Belief: Given Y, Y^a, Y^b it is difficult to compute Y^{ab}.

References

- **Introduction to Cryptography by Wade Trappe, Lawrence C Washington**
- **Lecture source:** https://courses.cs.washington.edu/courses/csep590/06wi/lectures/

Thanks for your attention !