Mật mã trên đường cong Elliptic Curves cho thiết bị IoT

Sinh viên thực hiện
Đặng Quang Trung - 20134145

Giảng viên hướng dẫn
TS Trần Vĩnh Đức

Ngày 17 tháng 5 năm 2018

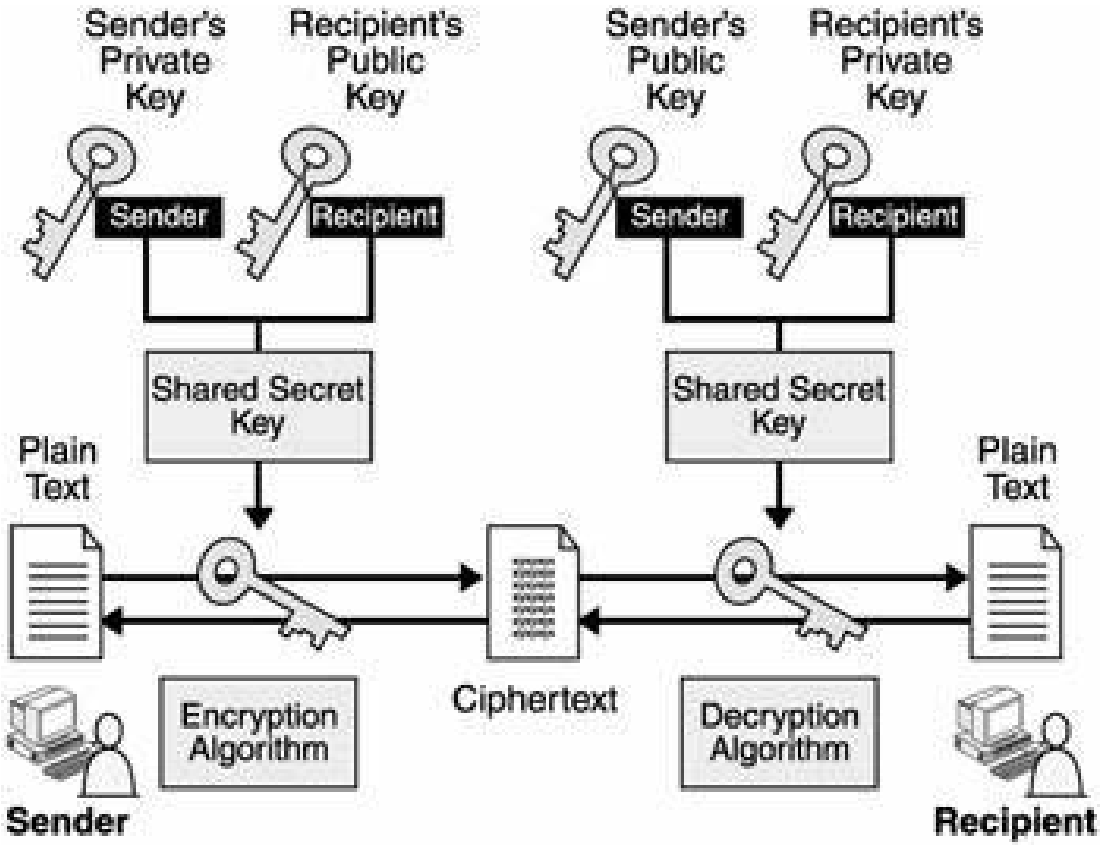
Nội dung trình bày

Tại sao cần có mật mã?

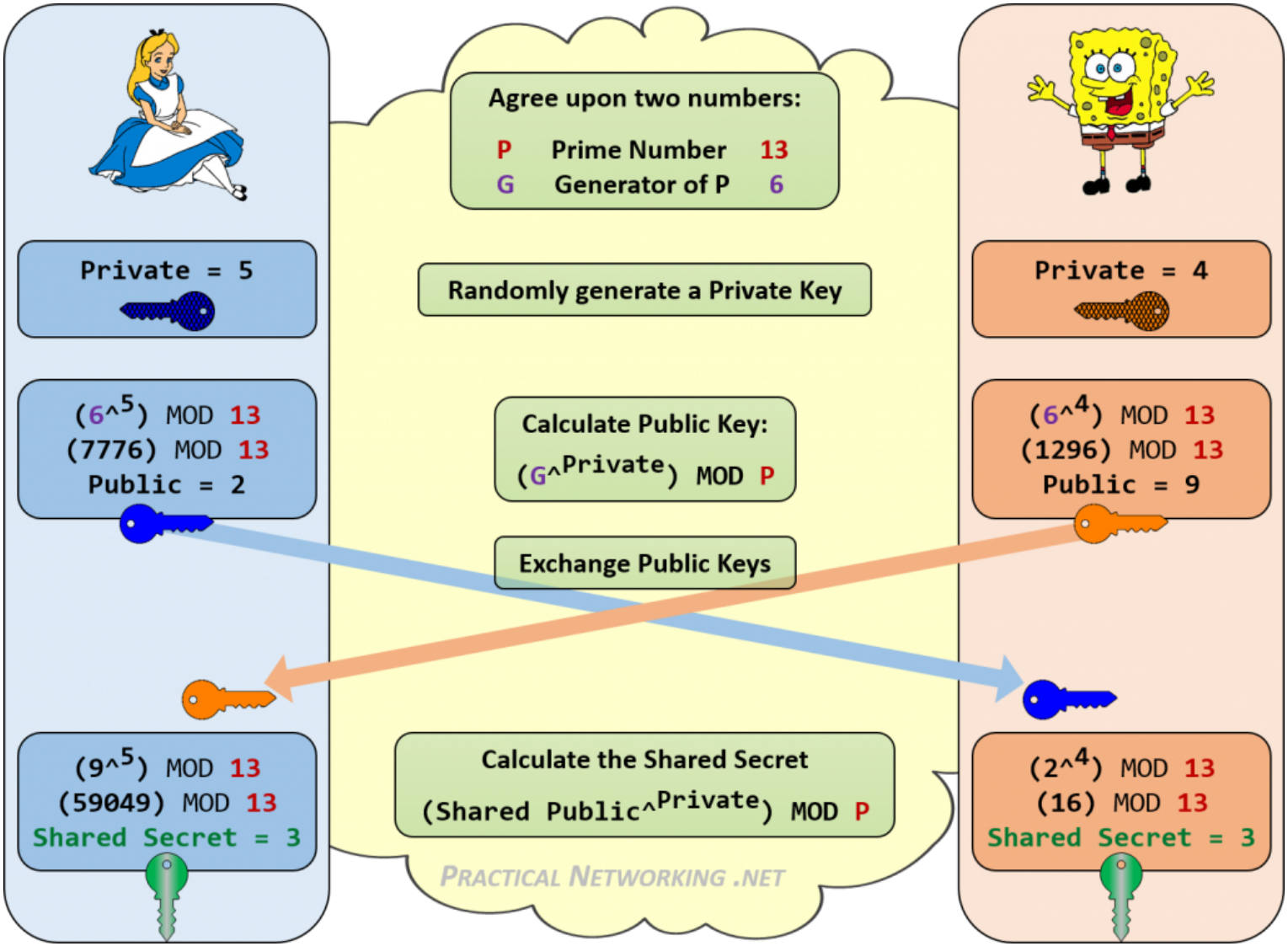
Ứng dụng

- Thương mại điện tử:
  - Chữ ký điện tử.
  - Mã hóa thông tin giao dịch.
- Mạng xã hội:
  - Mã hóa tin nhắn, văn bản,thư điện tử, ...
- Banking
  - Xác thực người dùng
  - Mã hóa giao dịch, thông tin khách hàng.
  - ....

Sơ đồ hệ mã khóa công khai



Diffe-Hellman



Định nghĩa

Một đường cong elliptic curve được xác định bởi phương trình đường cong

- **phương trình dạng Weierstrass**

$$E : y^2 = x^3 + Ax + B$$

với điều kiện $A, B \in \mathbb{F}$ thỏa mãn $4A^3 + 27B^2 \neq 0$.

- **phương trình dạng Montgomery**

$$M_{A,B} : By^2 = x^3 + Ax^2 + x$$

với điều kiện $A \in \mathbb{F} \setminus \{-2, 2\}, B \in \mathbb{F} \setminus \{0\}$ và $B(A^2 - 4) \neq 0$