CSE 539: Applied Cryptography
Week 7: RSA

Ni Trieu (ASU)

Reading: https://joyofcryptography.com/pdf/chap13.pdf
https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Recap: Hash Function

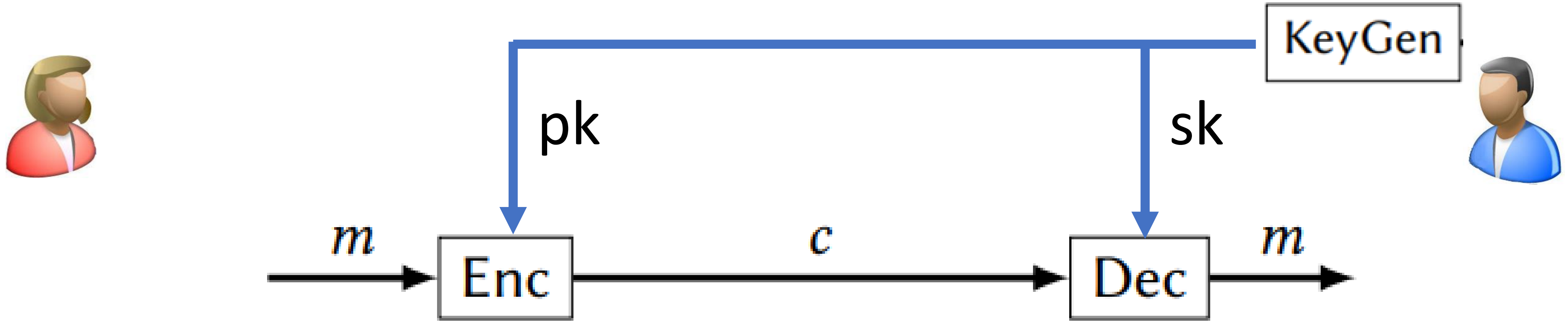
- A hash function maps a message of an arbitrary length to a n-bit output

$$\boldsymbol{H}: \{\boldsymbol{0}, \boldsymbol{1}\}^{*} \rightarrow \{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{n}}$$

- Collision resistance:
  - It should be hard to compute any collision $x \neq x'$ such that $H(x) = H(x')$

- Second-preimage resistance (weak collision resistant):
  - Given x, it should be hard to compute any collision involving x. In other words, it should be hard to compute $x' \neq x$ such that $H(x) = H(x')$

Public Key



RSA

- RSA = Ron Rivest, Adi Shamir, and Leonard Adleman
  - Developed in 1978
- RSA is an example of a public-key cryptosystem, and these are widely used today
  - Most Public Key Infrastructure (PKI) products.
  - SSL/TLS: Certificates and key-exchange.
  - Secure e-mail: PGP, Outlook,
- Encryption
- Decryption

RSA Math: Multiplicative Inverses

- The multiplicative inverse of x mod n is the integer y that satisfies xy = 1 (mod n) if such a number exists.
  - We usually refer to the multiplicative inverse of x as x^-1
- Example: Can we some y where 2y=1 mod (15)?

RSA Math: Multiplicative Inverses

- The multiplicative inverse of x mod n is the integer y that satisfies xy = 1 (mod n) if such a number exists.
  - We usually refer to the multiplicative inverse of x as x^-1
- Example: Can we some y where 3y=1 mod (15)?

RSA Math: Multiplicative Inverses

Which numbers have a multiplicative inverse mod n?

- x has a multiplicative inverse mod n if and only if gcd(x,n) = 1

- Why?
  - Bezout's Theorem:
    - For all integers x and y, there exist integers a and b such that ax + by = gcd(x,y).

How RSA works

The RSA function is defined as follows:

- Let p and q be distinct primes (later we will say more about how they are chosen), and let $N = pq$. N is called the **RSA modulus**.
- Let e and d be integers such that $ed \equiv_{\phi(N)} 1$. That is, e and d are multiplicative inverses mod $\phi(N)$ – not mod N!
- The RSA function is: $x \mapsto x^e \% N$, where $x \in \mathbb{Z}_N$.
- The inverse RSA function is: $y \mapsto y^d \% N$, where $x \in \mathbb{Z}_N$.

How RSA works

- Example:

How RSA works

- How to find e?