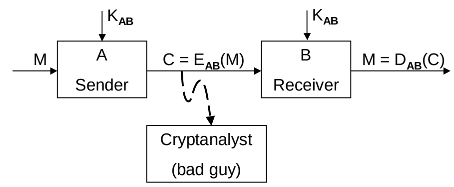
## Secret Codes

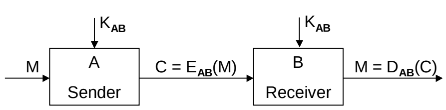


## What Is a Cryptosystem?



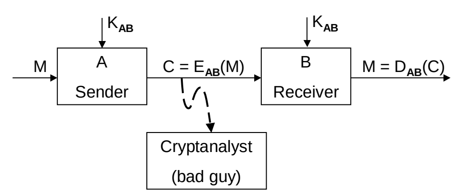



## What Is a Cryptosystem?



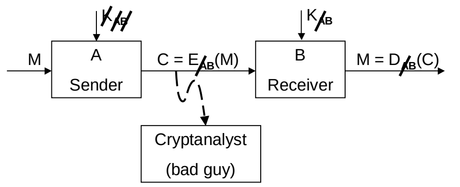



## What Is a Cryptosystem?




| M | C | $K_{AB}$ |
|---|---|---|
| Message | Encryption | Key |
| Plaintext | Cyphertext | |
| Cleartext | | |

## What Is a Public Key Cryptosystem?




| M | C | $K_B$ | $E_B$ |
|---|---|---|---|
| Message | Encryption | Key | Public Key |
| Plaintext | Cyphertext | Private Key | |
| Cleartext | | | |



## Receiver's Set-Up

- ❖ Choose 500-digit primes $p$ and $q$,
  with $p \equiv 2 \pmod 3$ and $q \equiv 2 \pmod 3$
  $p = 5$, $q = 11$



## The RSA Public Key Cryptosystem

- ❖ Invented by Rivest, Shamir, and Adleman in 1977.
- ❖ Has proven resistant to all cryptanalytic attacks.



## Receiver's Set-Up

- ❖ Choose 500-digit primes $p$ and $q$,
  with $p \equiv 2 \pmod 3$ and $q \equiv 2 \pmod 3$
  $p = 5$, $q = 11$
- ❖ Let $n = pq$.
  $n = 55$

## Receiver’s Set-Up

- Choose 500-digit primes $p$ and $q$,
  with $p \equiv 2 \pmod 3$ and $q \equiv 2 \pmod 3$
  $p = 5$, $q = 11$
- Let $n = pq$.
  $n = 55$
- Let $s = (1/3)\ (2(p - 1)(q - 1) + 1)$.
  $s = (1/3)\ (2 \cdot 4 \cdot 10 + 1) = 27$



## Encrypting a Message

- Break the message into chunks.
  H I  C H R I S ...



## Receiver’s Set-Up

- Choose 500-digit primes $p$ and $q$,
  with $p \equiv 2 \pmod 3$ and $q \equiv 2 \pmod 3$
  $p = 5$, $q = 11$
- Let $n = pq$.
  $n = 55$
- Let $s = (1/3)\ (2(p - 1)(q - 1) + 1)$.
  $s = (1/3)\ (2 \cdot 4 \cdot 10 + 1) = 27$
- Publish $n$.
  Keep $p$, $q$, and $s$ secret.



## Encrypting a Message

- Break the message into chunks.
  $\boxed{H}\boxed{I}$ $\boxed{C}\boxed{H}\boxed{R}\boxed{I}\boxed{S}$ ...

## Encrypting a Message

- Break the message into chunks.
  H I  C H R I S ...

- Translate each chunk into an integer $M$ ($0 \leq M < n$) by any convenient method.
  8 9  3 8 18 9 19 ...



## Decrypting a Cyphertext C

- Let $D(C) = C^s \bmod n$.
  $C = 17$, $n = 55$, $s = 27$
  $17^{27} = 1{,}667{,}711{,}322{,}168{,}688{,}287{,}513{,}535{,}727{,}415{,}473$
  $= 30{,}322{,}024{,}039{,}430{,}696{,}136{,}609{,}740{,}498{,}463 \times 55 + 8$
  $D(17) = 8$



## Encrypting a Message

- Break the message into chunks.
  H I  C H R I S ...

- Translate each chunk into an integer $M$ ($0 \leq M < n$) by any convenient method.
  8 9  3 8 18 9 19 ...

- Let $E(M) = M^3 \bmod n$.
  $M = 8$, $n = 55$
  $8^3 = 512 = 9 \times 55 + 17$
  $E(8) = 17$



## Decrypting a Cyphertext C

- Let $D(C) = C^s \bmod n$.
  $C = 17$, $n = 55$, $s = 27$
  $17^{27} = 1{,}667{,}711{,}322{,}168{,}688{,}287{,}513{,}535{,}727{,}415{,}473$
  $= 30{,}322{,}024{,}039{,}430{,}696{,}136{,}609{,}740{,}498{,}463 \times 55 + 8$
  $D(17) = 8$

- Translate $D(C)$ into letters.
  H

## Decrypting a Cyphertext C Efficiently

- $C = 17$, $n = 55$, $s = 27$

$17^2 \equiv 289 \equiv 14 \pmod{55}$

$17^4 \equiv 17^2 \bullet 17^2 \equiv 14 \bullet 14 \equiv 196 \equiv 31 \pmod{55}$

$17^8 \equiv 17^4 \bullet 17^4 \equiv 31 \bullet 31 \equiv 961 \equiv 26 \pmod{55}$

$17^{16} \equiv 17^8 \bullet 17^8 \equiv 26 \bullet 26 \equiv 676 \equiv 16 \pmod{55}$

$17^{27} \equiv 17^{16} \bullet 17^8 \bullet 17^2 \bullet 17^1 \equiv 16 \bullet 26 \bullet 14 \bullet 17 \equiv 416 \bullet 14 \bullet 17 \equiv 31 \bullet 14 \bullet 17 \equiv 434 \bullet 17 \equiv (-6) \bullet 17 \equiv -102 \equiv 8 \pmod{55}$

$D(17) = 8$



## Why Does It Work?

**Euler's Theorem** (1736): Suppose

- $p$ and $q$ are distinct primes,
- $n = pq$,
- $0 \leq M < n$, and
- $k > 0$.

Then $M^{k(p-1)(q-1)+1} \bmod n = M$.

$$(M^3)^s = (M^3)^{(1/3)(2(p-1)(q-1)+1)}$$
$$= M^{2(p-1)(q-1)+1} \equiv M \pmod{n}$$



## Why Does It Work?

**Euler's Theorem** (1736): Suppose

- $p$ and $q$ are distinct primes,
- $n = pq$,
- $0 \leq M < n$, and
- $k > 0$.

Then $M^{k(p-1)(q-1)+1} \bmod n = M$.



## Leonhard Euler 1707-1783

## Why Is It Secure?

- To find $M = D(C)$, you seem to need $s$.



## Why Is It Secure?

- To find $M = D(C)$, you seem to need $s$.
- To find s, you seem to need $p$ and $q$.
- All the cryptanalyst has is $n = pq$.



## Why Is It Secure?

- To find $M = D(C)$, you seem to need $s$.
- To find s, you seem to need $p$ and $q$.



## Why Is It Secure?

- To find $M = D(C)$, you seem to need $s$.
- To find s, you seem to need $p$ and $q$.
- All the cryptanalyst has is $n = pq$.
- How hard is it to factor a 1000-digit number $n$?
  With the grade school method,
  doing 1,000,000,000 steps per second
  it would take …

## Why Is It Secure?

- To find *M = D(C),* you seem to need *s.*
- To find s, you seem to need *p* and *q.*
- All the cryptanalyst has is $n = pq$.
- How hard is it to factor a 1000-digit number *n*?
  With the grade school method,
  doing 1,000,000,000 steps per second
  it would take … $10^{483}$ years.



## State of the Art in Factoring

- 1977: Inventors encrypt a challenge using “RSA129,” a 129-digit number $n = pq$.
- 1981: Pomerance invents Quadratic Sieve factoring method.
- 1994: Using Quadratic Sieve, RSA129 is factored over 8 months using 1000 computers on the Internet around the world.
- 1999: Using a new method, RSA140 is factored.
- Using Quadratic Sieve, a 250-digit number would take 800,000,000 months instead of 8.



## State of the Art in Factoring

- 1977: Inventors encrypt a challenge using “RSA129,” a 129-digit number $n = pq$.
- 1981: Pomerance invents Quadratic Sieve factoring method.
- 1994: Using Quadratic Sieve, RSA129 is factored over 8 months using 1000 computers on the Internet around the world.
- 1999: Using a new method, RSA140 is factored.