Information & System Security

Lecture 29

VIT-AP UNIVERSITY

Asymmetric

or

Public Key

Cryptography

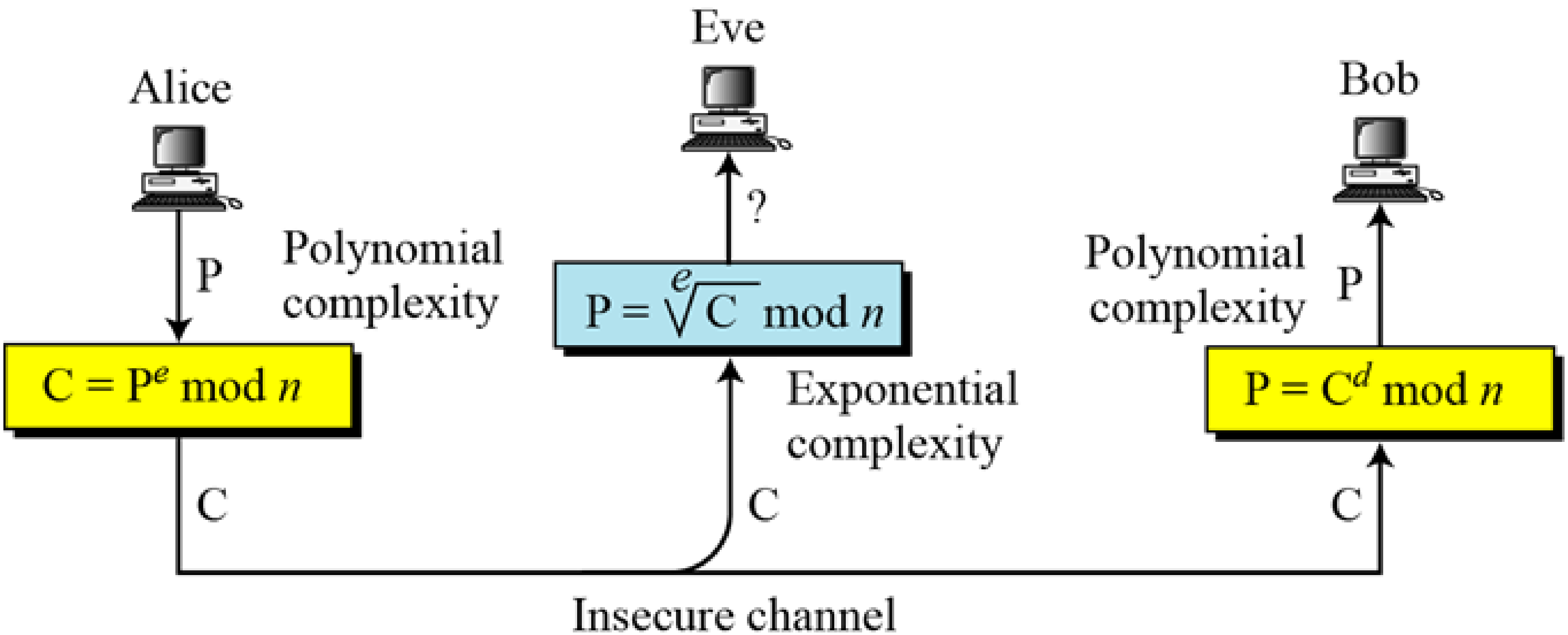
10-2 RSA CRYPTOSYSTEM

The most common public-key algorithm is the RSA cryptosystem, named for its inventors (Rivest, Shamir, and Adleman, 1977).

Topics discussed in this section:

10.2.1 Introduction
10.2.2 Procedure
10.2.3 Some Trivial Examples

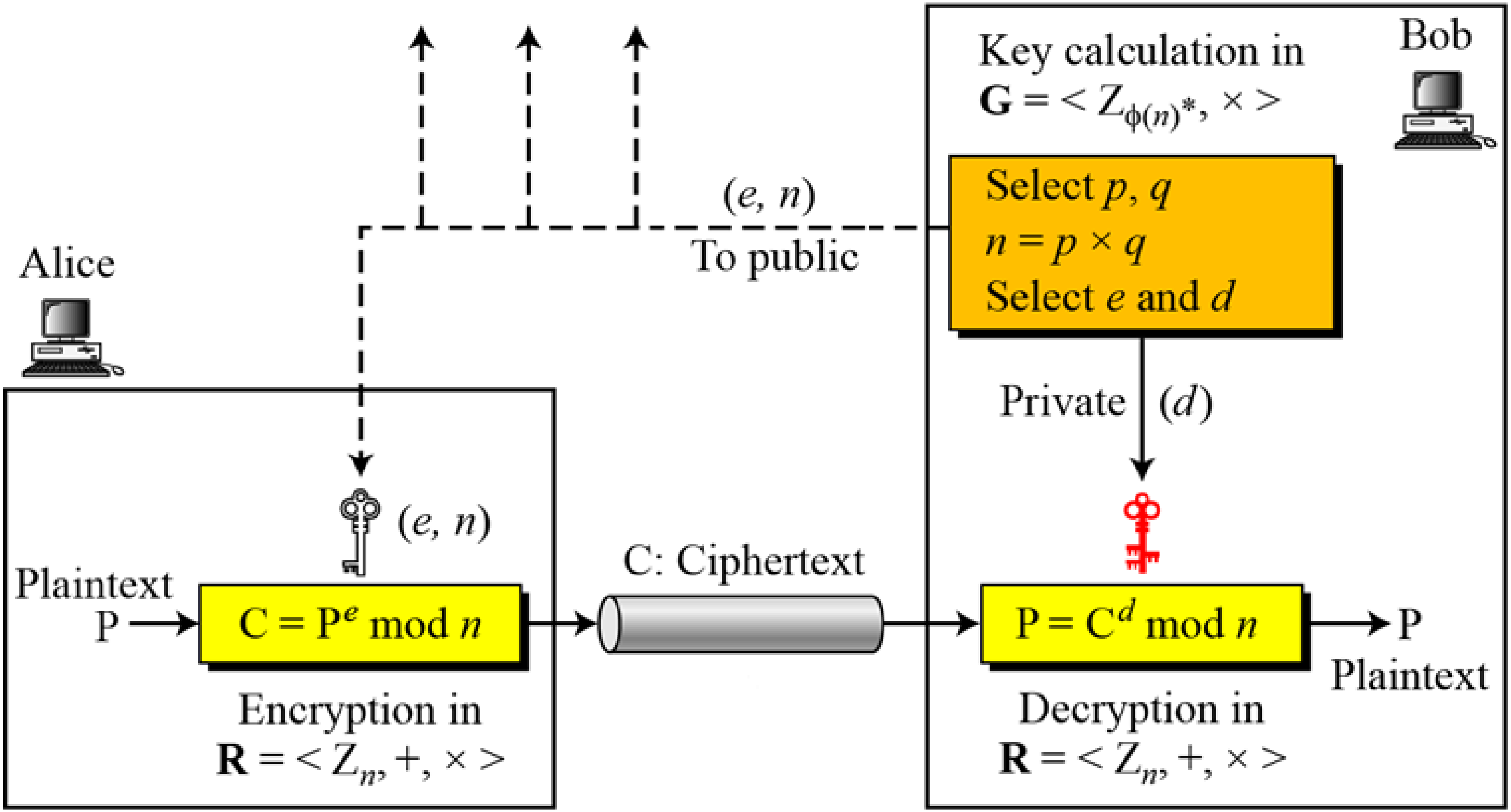
10.2.1 Introduction



Complexity of operations in RSA

RSA uses modular exponentiation for encryption/decryption;
To attack it, Eve needs to calculate $\sqrt[e]{C} \bmod n$.

10.2.2 Procedure



Encryption, decryption, and key generation in RSA

10.2.2 Continued

Two Algebraic Structures

Encryption/Decryption Ring: $\boxed{R = \langle Z_n, +, \times \rangle}$

Key-Generation Group: $\boxed{G = \langle Z^*_{\phi(n)}, \times \rangle}$

RSA uses two algebraic structures:
a public ring $R = \langle Z_n, +, \times \rangle$ and a private group $G = \langle Z^*_{\phi(n)}, \times \rangle$.

In RSA, the tuple (e, n) is the public key; the integer d is the private key.

10.2.2 Continued

RSA_Key_Generation

{

Select two large primes p and q such that $p \neq q$.

$n \leftarrow p \times q$

$\phi(n) \leftarrow (p - 1) \times (q - 1)$

Select e such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$

$d \leftarrow e^{-1} \bmod \phi(n)$ // d is inverse of e modulo $\phi(n)$

Public_key $\leftarrow$ (e, n) // To be announced publicly

Private_key $\leftarrow d$ // To be kept secret

return Public_key and Private_key

}

10.2.2 Continued

Encryption

```
RSA_Encryption (P, e, n)
{    // P is the plaintext in Z_n and P < n
     C ← Fast_Exponentiation (P, e, n)
     return C     // Calculation of (P^e mod n)
}
```

In RSA, *p* and *q* must be at least 512 bits; *n* must be at least 1024 bits.

Decryption

```
RSA_Decryption (C, d, n)
{   //C is the ciphertext in Z_n
     P ← Fast_Exponentiation (C, d, n)
     return P   // Calculation of (C^d mod n)
}
```

Proof of RSA

If $n = p \times q$, $a < n$, and k is an integer, then $a^{k \times \phi(n)+1} \equiv a \pmod{n}$.

$P_1 = C^d \bmod n = (P^e \bmod n)^d \bmod n = P^{ed} \bmod n$

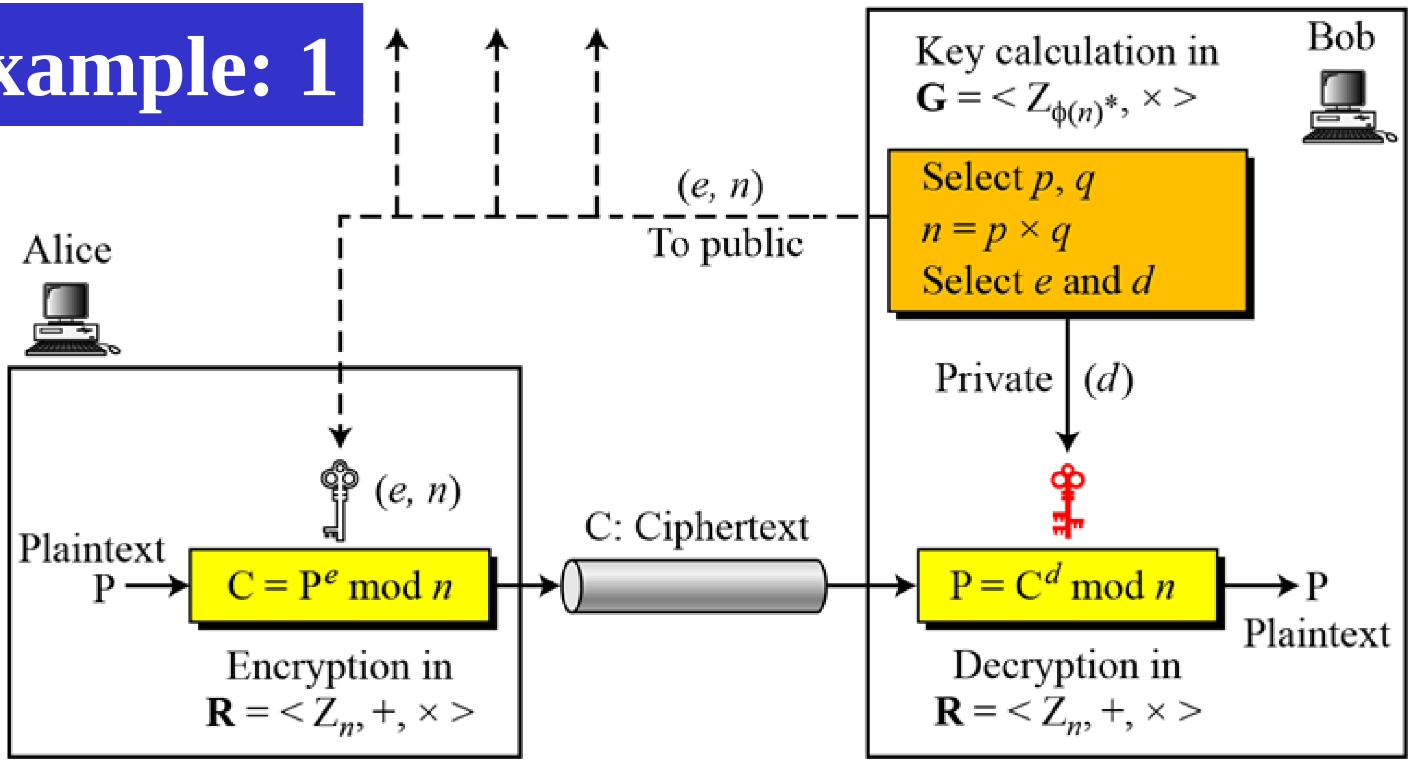
$ed = k\phi(n) + 1$ // d and e are inverses modulo $\phi(n)$

$P_1 = P^{ed} \bmod n \;\rightarrow\; P_1 = P^{k\phi(n)+1} \bmod n$

$P_1 = P^{k\phi(n)+1} \bmod n = P \bmod n$ // Euler's theorem (second version)

10.2.3 Some Trivial Examples of RSA PKC

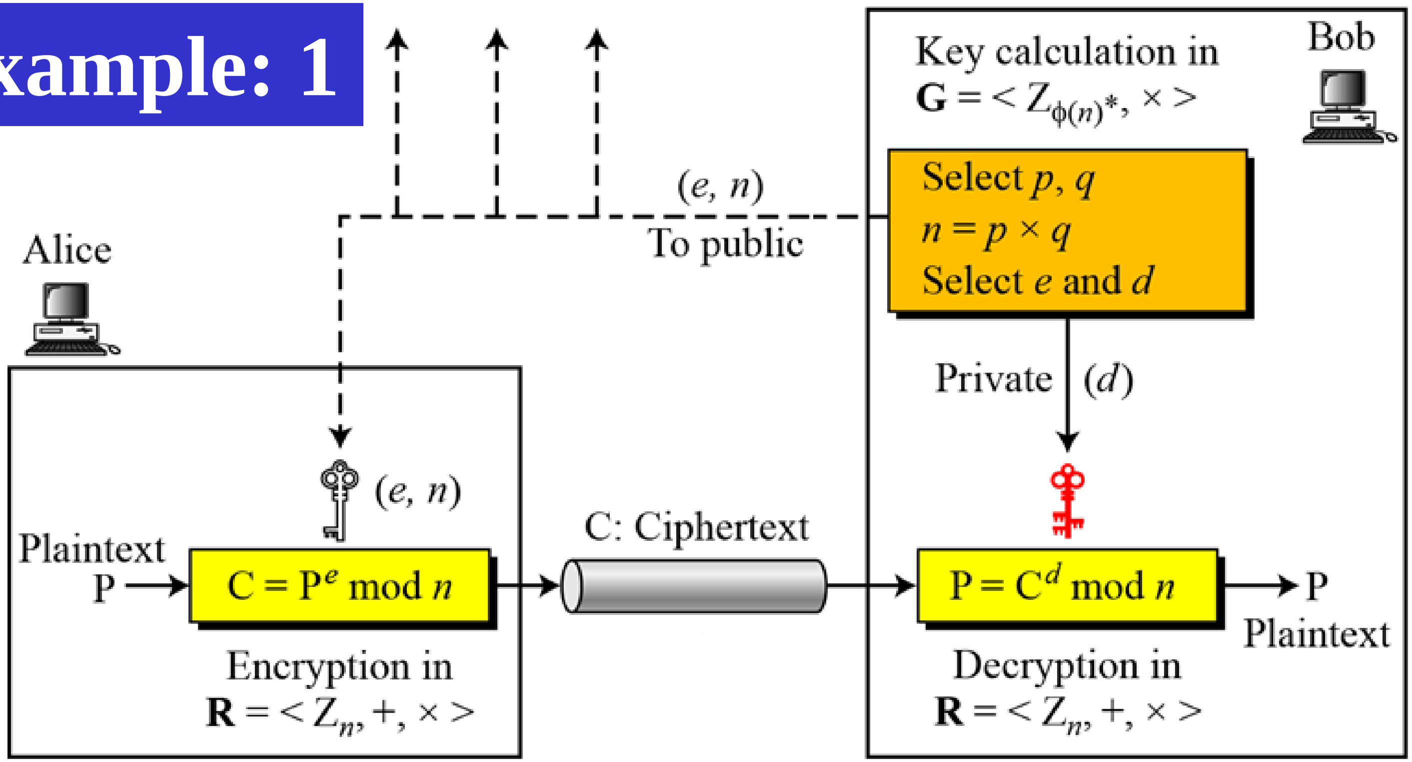
Example: 1



Bob chooses p=3 and q=5. n=? ϕ(n)=**?**. If he chooses e from $Z^*_{\emptyset(n)}$ to be 3, then finds d=**?**. Now Alice wants to send the plaintext P=2 to Bob. She uses the public exponent e to encrypt 2 and finds ciphertext C=**?**. How Bob will find plaintext P from C?

10.2.3 Continued

Example: 1



Solution:

$n = p.q = 3x5 = 15$. $\phi(n) = \phi(p.q) = \phi(p) \times \phi(q) = 2 \times 4 = 8$. $e = 3$, $P=2$.

$d = e^{-1} \bmod \phi(n) = 3^{-1} \bmod 8 = 3$.

Public Key: $(e,n) = (3,15)$ and Private Key: $d = 3$.

Alice-Encryption: $C = P^e \bmod n = 2^3 \bmod 15 = 8$.

Bob-Decryption: $P = C^d \bmod n = 8^3 \bmod 15 = 512 \bmod 15 = 2$.

10.2.3 Continued

Example: 2

Bob chooses 7 and 11 as p and q and calculates n = 77. The value of $\phi(n) = (7 - 1)(11 - 1)$ or 60. Now he chooses two exponents, e and d, from $Z_{60}*$. If he chooses e to be 13, then d is 37. Note that $e \times d$ mod 60 = 1 (they are inverses of each Now imagine that Alice wants to send the plaintext 5 to Bob. She uses the public exponent 13 to encrypt 5.

Plaintext: 5 $\quad C = 5^{13} = 26 \bmod 77$ $\quad$ Ciphertext: 26

Bob receives the ciphertext 26 and uses the private key 37 to decipher the ciphertext:

Ciphertext: 26 $\quad P = 26^{37} = 5 \bmod 77$ $\quad$ Plaintext: 5

10.2.3 Continued

Example: 3

Now assume that another person, John, wants to send a message to Bob. John can use the same public key announced by Bob, 13; John’s plaintext is 63. John calculates the following:

Plaintext: 63 $\quad C = 63^{13} = 28 \bmod 77 \quad$ Ciphertext: 28

Bob receives the ciphertext 28 and uses his private key 37 to decipher the ciphertext:

Ciphertext: 28 $\quad P = 28^{37} = 63 \bmod 77 \quad$ Plaintext: 63

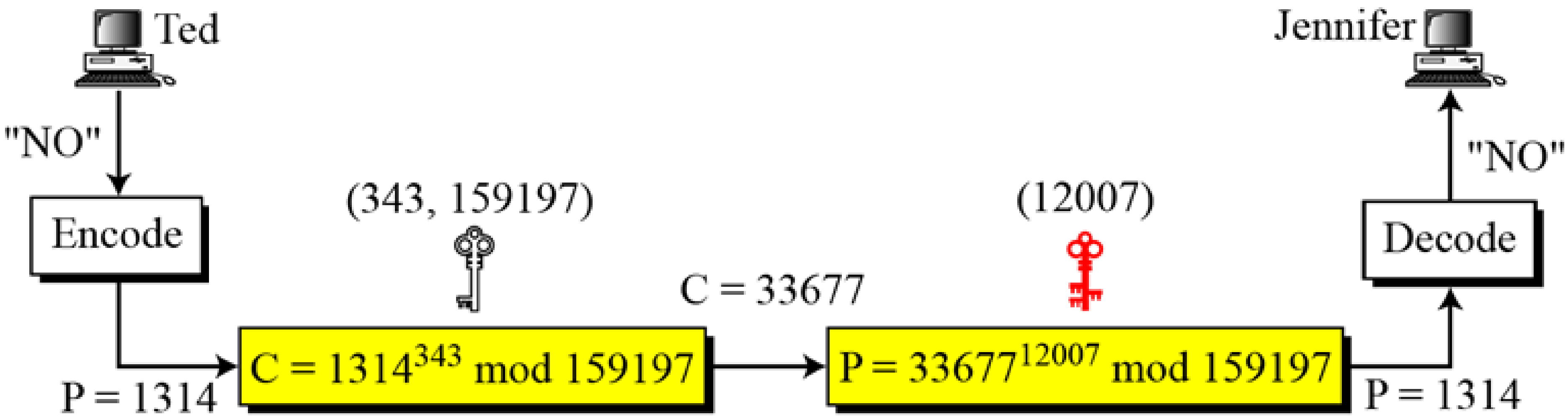
Example: 4

Jennifer creates a pair of keys for herself. She chooses p = 397 and q = 401. She calculates n = 159197. She then calculates $\phi(n)$ = 158400. She then chooses e = 343 and d = 12007. Show how Ted can send a message to Jennifer if he knows e and n.

Suppose Ted wants to send the message "NO" to Jennifer. He changes each character to a number (from 00 to 25), with each character coded as two digits. He then concatenates the two coded characters and gets a four-digit number. The plaintext is 1314.

10.2.3 Continued

Example: 4



Encryption and decryption

10.2.5 Continued

Example: 5

Here is a more realistic example. We choose a 512-bit p and q, calculate n and $\phi(n)$, then choose e and test for relative primality with $\phi(n)$. We then calculate d. Finally, we show the results of encryption and decryption. The integer p is a 159-digit number.

$p =$ 96130345313583504574191581280615427909309845594996215822583150879647940455056470638491257160180347503120986660649242019180878066742
1096063354219926661209

$q =$ 120601919572314469182767942044508960015559250546370339360617983217314821484837646592153894532091752252732268301071206956046025138871
4552496900035966004561

Example: 5

The modulus $n = p \times q$. It has 309 digits.

n =	11593504173967614968892509864615887523771457375454144775485526137614788540832635081727687881596832516846884930062548576411125016241455233918292716250765677272746009708271412773043496050055634727456662806009992403710299142447229221577279853172703383938133469268413732762200096667667183183108837342082344437095 3

$\phi(n) = (p - 1)(q - 1)$ has 309 digits.

$\phi(n)$ =	11593504173967614968892509864615887523771457375454144775485526137614788540832635081727687881596832516846884930062548576411125016241455233918292716250765675105423360849291675203448262798811755478765701392344440571698958172819609822636107546721186461217135910735864061400888517026537727726446734106624385766412 8

10.2.5 Continued

Example: 5

Bob chooses e = 35535 (the ideal is 65537) and tests it to make sure it is relatively prime with φ(n). He then finds the inverse of *e* modulo φ(n) and calls it *d*.

e =	35535
d =	58008302860037763936093661289677917594669062089650962180422866111380593852822358731706286910030021710859044338402170729869087600611530620252495988444804756824096624708148581713046324064407770483313401085094738529564507193677406119732655742423721761767462077637164207600337085333288532144708859551366702948316

Example: 5

Alice wants to send the message "THIS IS A TEST", which can be changed to a numeric value using the 00−26 encoding scheme (26 is the space character).

P =	1907081826081826002619041819

The ciphertext calculated by Alice is $C = P^e$, which is

C =	475309123646226827206365550610545180942371796070491716523239243054
	452960613199328566617843418359114151119741125200568297979457173603 6
	1012782188478927415660904800235071907152771859149751888465888632101
	148354103361657898467968386763733765777465625079280521148141844048
	14184430812773059004692874248559166462108656

Example: 5

Bob can recover the plaintext from the ciphertext using $P = C^d$, which is

P =	1907081826081826002619041819

The recovered plaintext is “THIS IS A TEST” after decoding.

References

- **Chapter 10 -** Behrouz A Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, Mc Graw Hill, 3rd Edition, 2015.

- **Chapter 9 -** William Stallings, Cryptography and Network Security Principles and Practices, 7th Edition, Pearson Education, 2017.