6.1.
As we have seen in this chapter, public-key cryptography can be used for en- cryption and key exchange. Furthermore, it has some properties (such as nonrepu- diation) which are not offered by secret key cryptography.
So why do we still use symmetric cryptography in current applications?

Answer:
Symmetric cryptography helps us encrypt bulk data and is way faster than asymmetric cryptography, whereas we can always use asymmetric cryptographic encryption to wrap the symmetric key to facilitate integrity and non-repudiation.

6.2.
In this problem, we want to compare the computational performance of sym- metric and asymmetric algorithms. Assume a fast public-key library such as OpenSSL [132] that can decrypt data at a rate of 100 Kbit/sec using the RSA al- gorithm on a modern PC. On the same machine, AES can decrypt at a rate of 17 Mbit/sec. Assume we want to decrypt a movie stored on a DVD. The movie requires 1 GByte of storage. How long does decryption take with either algorithm?

Answer:
Decryption with RSA:
Speed of RSA = 100 kbits/s
Movie size = 1 GByte = 8 Gbits = 8 * 1000 * 1000 kbits
Time taken = 8 * 1000 * 1000 / 100 = 80, 000 s

Decryption with AES:
Speed with AES = 17 Mbits/s
Movie size = 1 GByte = 8 Gbits = 8 * 1000 Mbits
Time taken = 8 * 1000 / 17 = 470.58s ~= 471 s

6.3.
Assume a (small) company with 120 employees. A new security policy demands encrypted message exchange with a symmetric cipher. How many keys are required, if you are to ensure a secret communication for every possible pair of communicating parties?

Answer:
Because we need to choose 2 employees out of 120 for the security policy, we need to count how many distinct pairs of 2 are there in 120. This will be ${}^{120}C_2$ = 120*119/2*1 = 7140

6.5. Using the basic form of Euclid’s algorithm, compute the greatest common divisor of [For this problem use only a pocket calculator. Show every iteration step of Euclid’s algorithm, i.e., don’t write just the answer, which is only a number. Also, for every gcd, provide the chain of gcd computations, i.e., gcd(r0,r1) = gcd(r1,r2) = ··· .]

Answer:
1. 7469 and 2464
= gcd(7469, 2464)
= gcd(7469%2464, 2464)
= gcd(77,2464)
= gcd(2464%77, 77)
= gcd(0,77)
The greatest common divisor of 7469 and 2464 is 77

2. 2689 and 4001
= gcd(4001%2689, 2689)
= gcd(1312, 2689)
= gcd(2689%1312,1312)
= gcd(65, 1312)
= gcd(1312%65, 65)
= gcd(12, 65)

= gcd(65%12, 12)
= gcd(5,12)
= gcd(12%5, 5)
= gcd(2, 5)
= gcd(5%2, 2)
= gcd(1, 2)
= gcd(0, 1)
The greatest common divisor of 2689 and 4001 is 1

6.6.
Using the extended Euclidean algorithm, compute the greatest common divisor
and the parameters s,t of

Answer:
1. 198 and 243
= gcd(243, 198)
= gcd(243%198, 198)
= gcd(45, 198)
= gcd(198%45, 45)
= gcd(18, 45)
= gcd(45%18, 18)
= gcd(18, 9)
= gcd(18%9, 9)
= gcd(9, 0)
= 9

Writing equations for above

243 = 1*198 + 45
=> 45 = 243 - 1*198

198 = 4*45 + 18
=> 18 = 198 - 4*45
Replacing 45 from above
=> 18 = 198 - 4*(243-1*198)
=> 18 = 5*198 - 4*243

45 = 2*18 + 9
=> 9 = 45 - 2*18
Replacing 45 and 18 from above
=> 9 = 243 - 1*198 - 2*(5*198 - 4*243)
=> 9 = 9*243 - 11*198

So, s = 9 and t=-11

2. 1819 and 3587
= gcd(3587, 1819)
= gcd(3587%1819, 1819)
= gcd(1768, 1819)
= gcd(1819%1768, 1768)
= gcd(51, 1768)
= gcd(1768%51, 51)
= gcd(34, 51)
= gcd(51%34, 34)
= gcd(17, 34)
= gcd(34%17, 17)

= gcd(0, 17)
17

Writing equations for above

3587 = 1*1819 + 1768
=> 1768 = 3587 - 1*1819

1819 = 1*1768 + 51
=> 51 = 1819 - 1*1768
Relacing 1768 from above
=> 51 = 1819 - 1*(3587 - 1*1819)
=> 51 = 2*1819 - 1*3587

1768 = 34*51 + 34
=> 34 = 1768 - 34*51
Replacing 1768 and 51 from above
=> 34 = 3587 - 1*1819 - 34*(2*1819 - 1*3587)
=> 34 = 35*3587 - 69*1819

51 = 1*34 + 17
=> 17 = 51 - 1*34
Replacing 51 and 34 from above
=> 17 = 2*1819 - 1*3587 - 1*(35*3587 - 69*1819)
=> 17 = 71*1819 - 36*3587
So, s = -36 and t = 71

For every problem check if s r0 + t r1 = gcd(r0 , r1) is actually fulfilled. The rules are the same as above: use a pocket calculator and show what happens in every iteration step.

6.7.
With the Euclidean algorithm we finally have an efficient algorithm for finding the multiplicative inverse in Zm that is much better than exhaustive search. Find the inverses in Zm of the following elements a modulo m:
Note that the inverses must again be elements in Zm and that you can easily verify your answers.

Answer:
1. a = 7, m = 26 (affine cipher)
Writing equations for EEA
26 = 3*7 + 5
=> 5 = 26 - 3*7

7 = 1*5 + 2
=> 2 = 7 - 1*5
Replacing 5 from above
=> 2 = 7 - 1*(26-3*7)
=> 2 = 4*7 - 1*26

5 = 2*2 + 1
=> 1 = 5 - 2*2
Replacing 5 and 2 from above
=> 1 = 26 - 3*7 - 2*(4*7 - 1*26)
=> 1 = 3*26 -11*7

So, the multiplicative inverse of 7 is -11. And -11 ~= -11 + 26 = 15
So, 7^{-1} = 15
We can verify this is correct because 7*15 mod 26 = 105 mod 26 = 1

2. a = 19, m = 999

Writing equations for EEA

999 = 52*19 + 11
=> 11 = 999 - 52*19

19 = 1*11 + 8
=> 8 = 19 - 1*11
Replacing 11 from above
=> 8 = 19 - 1*(999 - 52*19)
=> 8 = 53*19 -1*999

11 = 1*8 + 3
=> 3 = 11 - 1*8
Replacing 11 and 8 from above
=> 3 = 999 - 52*19 - 1*(53*19 - 1*999)
=> 3 = 2*999 -105*19

8 = 2*3 + 2
=> 2 = 8 - 2*3
Replacing 8 and 3 from above
=> 2 = 53*19 -1*999 -2*(2*999 -105*19)
=> 2 = 263*19 -5*999

3 = 1*2 + 1
=> 1 = 3 - 1*2
Replacing 3 and 2 from above
=> 1 = 2*999 -105*19 - 1*(263*19 -5*999)
=> 1 = 7*999 - 368*19

So, the multiplicative inverse of 19 is -368. And -368 ~= -368 + 999 = 631 mod 999
So, 19^{-1} = 631
We can verify this is correct because 19*631 mod 999 = 1

6.8.
Determine φ (m), for m = 12, 15, 26, according to the definition: Check for each positive integer n smaller m whether gcd(n,m) = 1. (You do not have to apply Euclid’s algorithm.)

Answer:

For $m = 12$

Whereas m, i.e. 12, can be written in form.

$$12 = 2^2 \times 3^1$$

So, $\phi(12) = (2^2 - 2^1)(3^1 - 3^0)$

$= (4 - 2)(3 - 1)$

$= (2)(2)$

$= 4$

Solving according to the definition for 12

$Z_{12} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]$

gcd(0, 12) = 12
gcd(1, 12) = 1 *
gcd(2, 12) = 2
gcd(3, 12) = 3
gcd(4, 12) = 4
gcd(5, 12) = 1 *
gcd(6, 12) = 6
gcd(7, 12) = 1 *
gcd(8, 12) = 4
gcd(9, 12) = 3
gcd(10, 12) = 2
gcd(11, 12) = 1 *

Therefore, 4 no.'s in Z_{12} has gcd 1

So $\phi(12) = 4$

For $m = 15$

$Z_{15} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]$

gcd(0, 15) = 15
gcd(1, 15) = 1 *
gcd(2, 15) = 1 *
gcd(3, 15) = 3
gcd(4, 15) = 1 *
gcd(5, 15) = 5
gcd(6, 15) = 3
gcd(7, 15) = 1 *
gcd(8, 15) = 1 *
gcd(9, 15) = 3
gcd(10, 15) = 5
gcd(11, 15) = 1 *
gcd(12, 15) = 3
gcd(13, 15) = 1 *
gcd(14, 15) = 1 *

So, $\phi(15) = 8$

For $m = 26$

$Z_{26} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \ldots\ldots 25]$

gcd(0, 26) = 26
gcd(1, 26) = 1 *
gcd(2, 26) = 2
gcd(3, 26) = 1 *
gcd(4, 26) = 2
gcd(5, 26) = 1 *
gcd(6, 26) = 2
gcd(7, 26) = 1 *
gcd(8, 26) = 2
gcd(9, 26) = 1 *
gcd(10, 26) = 2
gcd(11, 26) = 1 *
gcd(12, 26) = 2
gcd(13, 26) = 13
gcd(14, 26) = 2
gcd(15, 26) = 1 *
gcd(16, 26) = 2
gcd(17, 26) = 1 *
gcd(18, 26) = 2
gcd(19, 26) = 1 *
gcd(20, 26) = 2
gcd(21, 26) = 1 *
gcd(22, 26) = 2
gcd(23, 26) = 1 *
gcd(24, 26) = 2
gcd(25, 26) = 1 *

So, $\phi(26) = 12$

6.9.

Develop formulae for φ (m) for the special cases when

Answer:
1. Since m is a prime number, then we don't need to break it down into further prime factors

So, $\varphi(m) = m^1 - m^0 = (m-1)$

2. m = p · q, where p and q are primes. This case is of great importance for the RSA cryptosystem. Verify your formula for m = 15,26 with the results from the previous problem.

$\varphi(m) = (p^1 - p^0)*(q^1 - q^0) = (p-1)(q-1)$
For m=15 = 3*5, applying above result, we get
φ (m) = (3-1)(5-1) = 2*4 = 8, which matches result from previous problem
For m=26 = 2*13, applying above result, we get
φ (m) = (2-1)(13-1) = 12, which matches result from previous problem

---