**•1. Người A,B chọn 2 số nguyên tố chung là g=2 , p = 997, a=47, b= 43. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman.**

A và B thỏa thuận sử dụng chung 2 số p = 997 và g = 2.

A chọn 1 số nguyên bí mật a = 47 và gửi cho B giá trị A = g^a mod p

=> A = 2^47 mod 997 = (2^33 mod 997) \* (2^14 mod 997) = (935\*432) mod 997 =  135

B chọn 1 số nguyên bí mật b = 43 và gửi cho A giá trị B = g^b mod p

=> B = 2^43 mod 997 = (2^33 mod 997) \* (2^10 mod 997) = (935\*27) mod 997 = 320

A tính s = B^a mod p = 320^47 mod 997 = 370

B tính s = A^b mod p = 135^43 mod 997 = 370

**Vậy, khóa công khai là: (997,2) và (135,320)**

**Khóa bí mật là: A(47,370), B(43,370)**

**•2. Người A,B chọn 2 số nguyên tố chung là g=2 , p = 23, a=19, b=17. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B theo thuật mã Diffie-Hellman.**

A và B thỏa thuận sử dụng chung 2 số p = 23 và g = 2.

A chọn 1 số nguyên bí mật a = 19 và gửi cho B giá trị A = g^a mod p

=> A = 2^19 mod 23 =  3

B chọn 1 số nguyên bí mật b = 17 và gửi cho A giá trị B = g^b mod p

=> B = 2^17 mod 23 = 18

A tính s = B^a mod p = 18^19 mod 23 = 16

B tính s = A^b mod p = 3^17 mod 23 = 16

**Vậy, khóa công khai là: (23,2) và (3,18)**

**Khóa bí mật là: A(19,16), B(17,16)**

**•3. Theo thuật mã Diffie-Hellman RSA. Giả sử người A chọn các thông số  p =33, q =17, e = 13. Hỏi cặp khóa riêng của A là gì?**

N = p\*q = 33\*17 = 561

n = (p-1) \* (q-1) = 512

Ta có e = 13 là nguyên tố cùng nhau với n

Tính nghịch đảo của e trong phép modulo n được d = 315 (Vì 512\*8 - 13\*315 = 1)

**Khóa riêng của A = (d, N) = (315, 561).**

**•4. Theo thuật mã Diffie-Hellman, giả sử Alice & Bob chọn 2 số nguyên tố chung là g = 3, p = 353, với a=119, b=113 . Khóa riêng của Alice & Bob là ?**

A và B thỏa thuận sử dụng chung 2 số p = 353 và g = 3.

A chọn 1 số nguyên bí mật a = 119 và gửi cho B giá trị A = g^a mod p

=> A = 3^119 mod 353 = ((3^20 mod 353)^5) \* (3^19 mod 353) =((73^5 mod \* 353) \* 142) mod 353 =  (21\*142) mod 353 = 158

B chọn 1 số nguyên bí mật b = 113 và gửi cho A giá trị B = g^b mod p

=> B = 3^113 mod 353 = ((3^20 mod 353)^5) \* (3^13 mod 353) =((73^5 mod \* 353) \* 175) mod 353 =  (21\*175) mod 353 = 145

A tính s = B^a mod p = 145^119 mod 353 = 57

B tính s = A^b mod p = 158^113 mod 353 = 57

**Vậy, khóa công khai là: (353,3) và (119,113)**

**Khóa bí mật là: A(119,57), B(113,57)**

**•5. Cho bản mã y = 97, khóa riêng là p =31, q= 29, e =47. Khi giải mã bản mã y theo hệ RSA ta sẽ thu được bản rõ nào ?**

N = p\*q = 31\*29 = 899

n = (p-1) \* (q-1) = 840

Ta có e = 47 là nguyên tố cùng nhau với n

Tính nghịch đảo của e trong phép modulo n được d = 143

**Bản rõ là: x = y^d mod N = 97^143 mod 899 = 188.**

**•6.Cho bản rõ x = 82, khóa công khai n = 221, e = 37. Khi mã hóa bản rõ x với khóa trên theo hệ mã RSA ta sẽ thu được bản mã gì ?**

Tính nghịch đảo của e trong phép modulo n được d = 6 (Vì 37 \* 6 = 222)

Mã hóa bản rõ x = 82:

**Bản mã là: y = x^e mod n = 82^37 mod 221 = ((82^5 mod 221)^7 \* (82^2 mod 221) ) =  199**

**•7. Cho bản mã “VPTLJXAMJWVFKUBLJ” khóa k là “CITY”. Khi giải mã bản mã trên  với khóa k theo hệ mã Vigenere ta sẽ thu được bản rõ nào?**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| V | P | T | L | J | X | A | M | J | W | V | F | K | U | B | L | J |
| 21 | 15 | 19 | 11 | 9 | 23 | 0 | 12 | 9 | 22 | 21 | 5 | 10 | 20 | 1 | 11 | 9 |
| C | I | T | Y | C | I | T | Y | C | I | T | Y | C | I | T | Y | C |
| 2 | 8 | 19 | 24 | 2 | 8 | 19 | 24 | 2 | 8 | 19 | 24 | 2 | 8 | 19 | 24 | 2 |
| T | H | A | N | H | P | H | O | H | O | C | H | I | M | I | N | H |
| 19 | 7 | 0 | 13 | 7 | 15 | 7 | 14 | 7 | 14 | 2 | 7 | 8 | 12 | 8 | 13 | 7 |

**•8. Cho bản mã “YIVNQLTDF” khóa k là (23,29).Khi giải mã bản mã trên  với khóa k theo hệ mã Affine ta sẽ thu được bản rõ ?.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Y | I | V | N | Q | L | T | D | F |
| 24 | 8 | 21 | 13 | 16 | 11 | 19 | 3 | 5 |

Nghịch đảo của 23 theo module 26 là 17, ta có a^-1 = 17

Áp dụng hàm giải mã D(x) = (a^-1)(x-b) mod m = 17(x-29) mod 26, ta được dãy số:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| T | H | U | O | N | G | M | A | I |
| 19 | 7 | 20 | 14 | 13 | 6 | 12 | 0 | 8 |

**Kết quả là: THUONG MAI**

**•9. Cho bản mã “SKRQCFPDRN” khóa k là MONARCHY. Khi giải mã bản mã trên  với khóa k theo hệ mã Playfair ta sẽ thu được bản rõ  gì ?**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

Tiến hành tách bản mã thành các cặp như sau: SK RQ CF PD RN

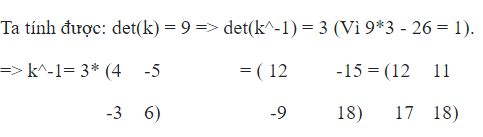
**=> Bản rõ là: TI NT HE TH AO => TIN THE THAO**

**•10. Cho bản mã “KRPKANHKPKKNUNOM” khóa k:**

**6      5**

**3      4**

Khi giải mã  với khóa k theo hệ mã Hill ta sẽ thu được  bản rõ nào ? Biết hàm mã y=kx ?



Giải mã:

C1 = “KR” = (10, 17) => C1 = (21, 8) => VI

C2 = “PK” = (15, 10) => C2 = (4, 19) => ET

C3 = “AN” = (0, 13) => C3 = (13, 0) => NA

C4 = “HK” = (7, 10) => C4 = (12, 13) => MN

C5 = “PK” = (15, 10) => C5 = (4, 19) => ET

C6 = “KN” = (10, 13) => C6 = (3, 14) => DO

C7 = “UN” = (20, 13) => C7 = (19, 2) => TC

C8 = “OM” = (14, 12) => C8 = (14, 12) => OM

**Kết quả là: VIET NAM NET DOT COM**

**•11.  Theo thuật mã Diffie-Hellman, giả sử  A  & B chọn 2 số nguyên tố chung là g = 2, p = 997, với a=131, b=151 . Tính khóa công khai, khóa riêng của của A & B ?**

A và B thỏa thuận sử dụng chung 2 số p = 997 và g = 2.

A chọn 1 số nguyên bí mật a = 131 và gửi cho B giá trị A = g^a mod p

=> A = 2^131 mod 997 = 398

B chọn 1 số nguyên bí mật b = 151 và gửi cho A giá trị B = g^b mod p

=> B = 2^151 mod 997 = 15

A tính s = B^a mod p = 15^131 mod 997 = 406

B tính s = A^b mod p = 398^151 mod 997 = 406

**Vậy, khóa công khai là: (997,2) và (398,15)**

**Khóa bí mật là: A(131,406), B(151,406)**

**•12. Người A chọn các thông số p =31, q =37, e = 119. Theo thuật mã RSA hỏi cặp khóa riêng và khóa công khai của A là gì ?  Trong trường hợp nhận được bản mã là 1091, các em  hãy tìm bản rõ ?**

N = 31\*37 = 1147

n = 1080

Ta có e = 119 là nguyên tố cùng nhau với n

Tính nghịch đảo của e trong phép modulo n được d = 599.

**Khóa công khai là: (119,1147)**

**Khóa riêng là: (599,1147)**

a có M = C^d mod N = 1091^599 mod 1147

1091^599 mod 1147 = ((1091^4 mod 1147)^149 mod 1147 \* 1091^3 mod 1147) mod 1147 = [(1) \*(2)]mod 1147

(1) <=> 1091^3 mod 1147 = 1298596571 mod 1147 = 1022

1091^4 mod 1147 = 1416768858961 mod 1147 = 118

(2)<=> 118^149 mod 1147 = ((118^6 mod 1147)^24 \* 118^5 mod 1147) mod 1147

118^5 mod 1147 = 22877577568 mod 1147 = 749

118^6 mod 1147 = 2699554153024 mod 1147 = 63

=> (63^24 mod 1147 = ((63^6 mod 1147)^4 mod 1147

63^6 mod 1147 = 62523502209 mod 1147 = 1

=>63^24 mod 1147 = (1^4) mod 1147 = 1

=>118^149 mod 1147 = (1 \* 749) mod 1147 = 749

**=>M = ((1)\*(2))mod1147 = (749\*1022) mod 1147 = 765478 mod 1147 = 429**

**Vậy bản rõ thu được là: 1091^599 mod 1147 = 429**

**•13. Cho bản mã “CLGSKOOUOUISOCSHBERU” khóa k là "CITY". Khi giải mã bản mã trên  với khóa k theo hệ mã Playfair ta sẽ thu được bản rõ  gì ?**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| C | I | T | Y | A |
| B | D | E | F | G |
| H | K | L | M | N |
| O | P | Q | R | S |
| U | V | W | X | Z |

Tiến hành tách bản mã thành các cặp: CL GS KO OU OU IS OC SH BE RU

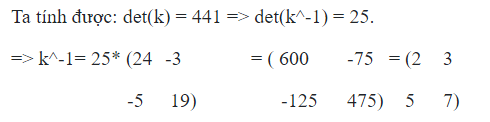
**=> Bản rõ là: TH AN HP HO HO AP HU ON GD OX => THANH PHO HOA PHUONG DO**

**•14. Cho bản mã “FJTQCQJCZHOIQM” khóa k:**

**19     3**

**5    24**

Khi giải mã  với khóa k theo hệ mã Hill ta sẽ thu được  bản rõ nào ? Biết hàm mã y=xk



Giải mã:

C1 = “FJ” = (5, 9) => C1 = (3, 0) => DA

C2 = “TQ” = (19, 16) => C2 = (14, 13) => ON

C3 = “CQ” = (2, 16) => C3 = (6, 14) => GO

C4 = “JC” = (9, 2) => C4 = (2, 15) => CP

C5 = “ZH” = (25, 7) => C5 = (7, 20) => HU

C6 = “OI” = (14, 8) => C7 = (16, 20) => QU

C7= “QM” = (16, 12) => C6 = (14, 2) => OC

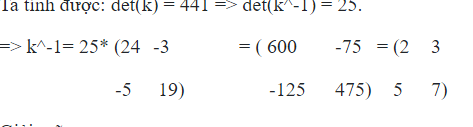
**Kết quả là: DAO NGOC PHU QUOC**

**•15. Cho bản mã “ZFUCTHFBTSXRWZ” khóa k:**

**19     3**

**5    24**

Khi giải mã  với khóa k theo hệ mã Hill ta sẽ thu được  bản rõ nào ? Biết hàm mã y=kx



Giải mã:

C1 = “ZF” = (25, 5) => C1 = (13, 4) => NE

C2 = “UC” = (20, 2) => C2 = (20, 10) => UK

C3 = “TH” = (19, 7) => C3 = (7, 14) => HO

C4 = “FB” = (5, 1) => C4 = (13, 6) => NG

**C5 = “TS” = (19, 18) => C5 = (14, 13) => ON**

**C6 = “XR” = (23, 17) => C7 = (19, 0) => TA**

**C7= “WZ” = (22, 25) => C6 = (15, 25) => PZ**

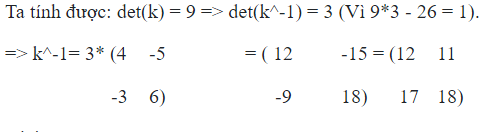
**Kết quả là: NEU KHONG ON TAP**

**•16. Cho bản mã “FTYICIGNSLFTHGFY” khóa k:**

**6      5**

**3      4**

**Khi giải mã  với khóa k theo hệ mã Hill ta sẽ thu được  bản rõ nào ? Biết hàm mã y=xk?**

****

Giải mã:

C1 = “FT” = (5,19) => C1 = (19, 7) => TH

C2 = “YI” = (24, 8) => C2 = (8, 18) => IS

C3 = “CI” = (2, 8) => C3 = (4, 10) => EK

C4 = “GN” = (6, 13) => C4 = (7, 14) => HO

C5 = “SL” = (18, 11) => C5 = (13, 6) => NG

C6 = “FT” = (5, 19) => C6 = (19, 7) => TH

C7 = “HG” = (7, 6) => C7 = (4, 3) => ED

C8 = “FY” = (5, 24) => C8 = (0, 19) => AT

**Kết quả là: THI SE KHONG THE DAT**

**•17.Cho k = 25, N = 26, giải mã văn bản, dùng  thuật mã Caesar:**

**với C = BZBDLBNFZMFNMSZO**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| B | Z | B | D | L | B | N | F | Z | M | F | N | M | S | Z | O |
| 1 | 25 | 1 | 3 | 11 | 1 | 13 | 5 | 25 | 12 | 5 | 13 | 12 | 18 | 25 | 14 |
| C | A | C | E | M | C | O | G | A | N | G | O | N | T | A | P |
| 2 | 0 | 2 | 4 | 12 | 2 | 14 | 6 | 0 | 13 | 6 | 14 | 13 | 19 | 0 | 15 |

**•18.Cho k = 23, N = 26, giải mã văn bản, dùng  thuật mã Caesar:**

**với   C = QEFAXQHBQNRX**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Q | E | F | A | X | Q | H | B | Q | N | R | X |
| 16 | 4 | 5 | 0 | 23 | 16 | 7 | 1 | 16 | 13 | 17 | 23 |
| T | H | I | D | A | T | K | E | T | Q | U | A |
| 19 | 7 | 8 | 3 | 0 | 19 | 10 | 4 | 19 | 16 | 20 | 0 |

**•19.Cho k = 24, N = 26, giải mã văn bản, dùng  thuật mã Caesar:**

**với   C = AFSAAYACKRFYLFAMLE**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | F | S | A | A | Y | A | C | K | R | F | Y | L | F | A | M | L | E |
| 0 | 5 | 18 | 0 | 0 | 24 | 0 | 2 | 10 | 17 | 5 | 24 | 11 | 5 | 0 | 12 | 11 | 4 |
| C | H | U | C | C | A | C | E | M | T | H | A | N | H | C | O | N | G |
| 2 | 7 | 20 | 2 | 2 | 0 | 2 | 4 | 12 | 19 | 7 | 0 | 13 | 7 | 2 | 14 | 11 | 6 |

**•20. Cho k = 19, N = 26, giải mã văn bản, dùng  thuật mã Caesar:**

**với   C = ZHHWURXTGWLXXRHN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Z | H | H | W | U | R | X | T | G | W | L | X | X | R | H | N |
| 25 | 7 | 7 | 22 | 20 | 17 | 23 | 19 | 6 | 22 | 11 | 23 | 23 | 17 | 7 | 13 |
| **G** | **O** | **O** | **D** | **B** | **Y** | **E** | **A** | **N** | **D** | **S** | **E** | **E** | **Y** | **O** | **U** |
| **6** | **14** | **14** | **3** | **1** | **24** | **4** | **0** | **13** | **3** | **18** | **4** | **4** | **24** | **14** | **20** |