**Bài tập thuật mã 5 - Thuật mã Affine**

**Nhóm 1**

* Hồ Phan Tấn Khoa
* Trần Minh Bảo Long
* Lê Văn Hiếu
* Phan Minh Thuận
* Trịnh Thanh Hải
* Nguyễn Minh Sang
* Phan Hoàng Triều
* Lê Trương Minh Hoàng

**Thuật mã Affine**

**Ta có k = (a, b) và N**

**Công thức mã hóa: C(x) = (ax + b) mod N**

**Công thức giải mã: P(x) = a^(-1)\*(x - b) mod N**

**với a^(-1) là nghịch đảo của a theo modulo N**

**a\*a^(-1) mod N = 1**

**Lưu ý: Trường hợp x < b thì ta có thể tính theo cách sau sao cho**

**0 < a^(-1)\*(x-b) + 26y <= 25 với y = |a^(-1)\*(x-b)| / 26**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **1. Cho k = (11, 6), N = 26, giải mã văn bản, dùng thuật mã Affine:**

**với C = CETUTUFYPFGTIYI**

**a = 11, b = 6**

**Ta có a^(-1) là nghịch đảo của a theo modulo n:**

**a\*a^(-1) mod 26 = 1 => a^(-1) = -7 + 26 = 19**

| **C =** | **C** | **E** | **T** | **U** | **T** | **U** | **F** | **Y** | **P** | **F** | **G** | **T** | **I** | **Y** | **I** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **2** | **4** | **19** | **20** | **19** | **20** | **5** | **24** | **15** | **5** | **6** | **19** | **8** | **24** | **8** |
| **a^(-1)(x-b) mod 26** | **2** | **14** | **13** | **6** | **13** | **6** | **7** | **4** | **15** | **7** | **0** | **13** | **12** | **4** | **12** |
| **P =** | **C** | **O** | **N** | **G** | **N** | **G** | **H** | **E** | **P** | **H** | **A** | **N** | **M** | **E** | **M** |

**Kết quả giải mã: P = CONGNGHEPHANMEM**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **2. Cho k = (17, 12), N = 26, mã hóa văn bản, dùng thuật mã Affine:**

**với P = CONGNGHETHONGTIN**

**a = 17, b = 12**

| **P =** | **C** | **O** | **N** | **G** | **N** | **G** | **H** | **E** | **T** | **H** | **O** | **N** | **G** | **T** | **I** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **2** | **14** | **13** | **6** | **13** | **6** | **7** | **4** | **19** | **7** | **14** | **13** | **6** | **19** | **8** | **13** |
| **(ax + b) mod 26** | **20** | **16** | **25** | **10** | **25** | **10** | **1** | **2** | **23** | **1** | **16** | **25** | **10** | **23** | **18** | **25** |
| **C =** | **U** | **Q** | **Z** | **K** | **Z** | **K** | **B** | **C** | **X** | **B** | **Q** | **Z** | **K** | **X** | **S** | **Z** |

**Kết quả mã hóa: C = UQZKZKBCXBQZKXSZ**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **3. Cho k = (21, 17), N = 26, mã hóa văn bản, dùng thuật mã Affine:**

**với P = TRUONGDAIHOCMO**

**a = 21 , b = 17**

| **P =** | **T** | **R** | **U** | **O** | **N** | **G** | **D** | **A** | **I** | **H** | **O** | **C** | **M** | **O** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **19** | **17** | **20** | **14** | **13** | **06** | **03** | **00** | **08** | **07** | **14** | **02** | **12** | **14** |
| **(ax + b) mod 26** | **00** | **10** | **21** | **25** | **04** | **13** | **02** | **17** | **03** | **08** | **25** | **07** | **09** | **25** |
| **C =** | **A** | **K** | **V** | **Z** | **E** | **N** | **C** | **R** | **D** | **I** | **Z** | **H** | **J** | **Z** |

**Kết quả mã hóa: C = AKVZENCRDIZHJZ**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **4. Cho k = (25, 29), N = 26, giải mã văn bản, dùng thuật mã Affine:**

**C = APWPDGJSFDQW**

**a = 25, b = 29**

**Ta có a^(-1) là nghịch đảo của a theo modulo n:**

**a\*a^(-1) mod 26 = 1 => a^(-1) = -1 + 26 = 25**

| **C =** | **A** | **P** | **W** | **P** | **D** | **G** | **J** | **S** | **F** | **D** | **Q** | **W** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **00** | **15** | **22** | **15** | **03** | **06** | **09** | **18** | **05** | **03** | **16** | **22** |
| **a^(-1)(x-b) mod 26** | **03** | **14** | **07** | **14** | **00** | **23** | **20** | **11** | **24** | **00** | **13** | **07** |
| **P =** | **D** | **O** | **H** | **O** | **A** | **X** | **U** | **L** | **Y** | **A** | **N** | **H** |

**Kết quả giải mã: P = DOHOAXULYANH**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **5. Cho k = (31, 12), N = 26, giải mã văn bản, dùng thuật mã Affine:**

**C = WEYEBIPAGI**

**a = 31, b = 12**

**Ta có a^(-1) là nghịch đảo của a theo modulo n:**

**a\*a^(-1) mod 26 = 1 => a^(-1) = -5 + 26 = 21**

| **C =** | **W** | **E** | **Y** | **E** | **B** | **I** | **P** | **A** | **G** | **I** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **22** | **4** | **24** | **4** | **1** | **8** | **15** | **0** | **6** | **8** |
| **a^(-1)(x-b) mod 26** | **2** | **14** | **18** | **14** | **3** | **20** | **15** | **8** | **4** | **20** |
| **P =** | **C** | **O** | **S** | **O** | **D** | **U** | **L** | **I** | **E** | **U** |

**Kết quả giải mã: P = COSODULIEU**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **6. Cho k = (31, 24), N = 26, mã hóa văn bản, dùng thuật mã Affine:**

**với P = MANCHESTERUNITED**

**a = 31 , b = 24**

| **P =** | **M** | **A** | **N** | **C** | **H** | **E** | **S** | **T** | **E** | **R** | **U** | **N** | **I** | **T** | **E** | **D** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **12** | **00** | **13** | **02** | **07** | **04** | **18** | **19** | **04** | **17** | **20** | **13** | **08** | **19** | **04** | **03** |
| **(ax + b) mod 26** | **06** | **24** | **11** | **08** | **07** | **18** | **10** | **15** | **18** | **05** | **20** | **11** | **12** | **15** | **18** | **13** |
| **C =** | **G** | **Y** | **L** | **I** | **H** | **S** | **K** | **P** | **S** | **F** | **U** | **L** | **M** | **P** | **S** | **N** |

**Kết quả mã hóa: C = GYLIHSKPSFULMPSN**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **7. Cho k = (31, 24), N = 26, giải mã văn bản, dùng thuật mã Affine:**

**C = DYOSFLGULMIHXI**

**a = 31 , b = 24**

**Ta có a^(-1) là nghịch đảo của a theo modulo n:**

**a\*a^(-1) mod 26 = 1 => a^(-1) = -5 + 26 = 21**

| **C =** | **D** | **Y** | **O** | **S** | **F** | **L** | **G** | **U** | **L** | **M** | **I** | **H** | **X** | **I** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **03** | **24** | **14** | **18** | **05** | **11** | **06** | **20** | **11** | **12** | **08** | **07** | **23** | **08** |
| **a^(-1)(x-b) mod 26** | **01** | **00** | **24** | **4** | **17** | **13** | **12** | **20** | **13** | **08** | **02** | **07** | **05** | **02** |
| **P =** | **B** | **A** | **Y** | **E** | **R** | **N** | **M** | **U** | **N** | **I** | **C** | **H** | **F** | **C** |

**Kết quả giải mã: P = BAYERNMUNICHFC**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **8. Cho k = (41, 35), N = 26, giải mã văn bản, dùng thuật mã Affine:**

**C = ERJSTLNZRCJCMTYJENJ**

**a = 41, b = 35**

**Ta có a^(-1) là nghịch đảo của a theo modulo n:**

**a\*a^(-1) mod 26 = 1 => a^(-1) = 7**

| **C =** | **E** | **R** | **J** | **S** | **T** | **L** | **N** | **Z** | **R** | **C** | **J** | **C** | **M** | **T** | **Y** | **J** | **E** | **N** | **J** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **04** | **17** | **09** | **18** | **19** | **11** | **13** | **25** | **17** | **02** | **09** | **02** | **12** | **19** | **24** | **09** | **04** | **13** | **09** |
| **a^(-1)(x-b) mod 26** | **17** | **04** | **00** | **11** | **18** | **14** | **02** | **08** | **04** | **03** | **00** | **03** | **21** | **18** | **01** | **00** | **17** | **02** | **00** |
| **P =** | **R** | **E** | **A** | **L** | **S** | **O** | **C** | **I** | **E** | **D** | **A** | **D** | **V** | **S** | **B** | **A** | **R** | **C** | **A** |

**Kết quả giải mã: P = REALSOCIEDADVSBARCA**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **9. Cho k = (53, 21), N = 26, giải mã văn bản, dùng thuật mã Affine:**

**C = ODIOPXFCJVCJXFDOCPVO**

**a = 53, b = 21**

**Ta có a^(-1) là nghịch đảo của a theo modulo n:**

**a\*a^(-1) mod 26 = 1 => a^(-1) = 1**

| **C =** | **O** | **D** | **I** | **O** | **P** | **X** | **F** | **C** | **J** | **V** | **C** | **J** | **X** | **F** | **D** | **O** | **C** | **P** | **V** | **O** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **14** | **03** | **08** | **14** | **15** | **23** | **05** | **02** | **09** | **21** | **02** | **09** | **23** | **05** | **03** | **14** | **02** | **15** | **21** | **14** |
| **a^(-1)(x-b) mod 26** | **19** | **08** | **13** | **19** | **20** | **02** | **10** | **07** | **14** | **00** | **07** | **14** | **02** | **10** | **08** | **19** | **07** | **20** | **00** | **19** |
| **P =** | **T** | **I** | **N** | **T** | **U** | **C** | **K** | **H** | **O** | **A** | **H** | **O** | **C** | **K** | **I** | **T** | **H** | **U** | **A** | **T** |

**Kết quả giải mã: P =TINTUCKHOAHOCKYTHUAT**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* **10. Cho k = (53, 47), N = 26, giải mã văn bản, dùng thuật mã Affine:**

**C = OCPJIBICVPGTOJCJIB**

**a = 53 , b = 47**

**Ta có a^(-1) là nghịch đảo của a theo modulo n:**

**a\*a^(-1) mod 26 = 1 => a^(-1) = 1**

| **C =** | **O** | **C** | **P** | **J** | **I** | **B** | **I** | **C** | **V** | **P** | **G** | **T** | **O** | **J** | **C** | **J** | **I** | **B** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **x =** | **14** | **02** | **15** | **09** | **08** | **01** | **08** | **02** | **21** | **15** | **06** | **19** | **14** | **09** | **02** | **09** | **08** | **01** |
| **a^(-1)(x-b) mod 26** | **19** | **07** | **20** | **14** | **13** | **06** | **13** | **07** | **00** | **20** | **11** | **24** | **19** | **14** | **07** | **14** | **13** | **06** |
| **P =** | **T** | **H** | **U** | **O** | **N** | **G** | **N** | **H** | **A** | **U** | **L** | **Y** | **T** | **O** | **H** | **O** | **N** | **G** |

**Kết quả giải mã: P =THUONGNHAULYTOHONG**