**Bài tập thuật mã 3 - Thuật mã Vigenere & Playfair**

**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

| 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 = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere :**

**với C = VPTLJXAMOWGEOW**

| **C** | **V** | **P** | **T** | **L** | **J** | **X** | **A** | **M** | **O** | **W** | **G** | **E** | **O** | **W** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **21** | **15** | **19** | **11** | **9** | **23** | **0** | **12** | **14** | **22** | **6** | **4** | **14** | **22** |
| **k** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** |
|  | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** |
| **(C - k) mod N** | **19** | **7** | **0** | **13** | **7** | **15** | **7** | **14** | **12** | **14** | **13** | **6** | **12** | **14** |
| **P** | **T** | **H** | **A** | **N** | **H** | **P** | **H** | **O** | **M** | **O** | **N** | **G** | **M** | **O** |

**Kết quả giải mã: P = THANH PHO MONG MO**

| 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 = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere :**

**với C = FIEYVVZYPPHY**

| **C** | **F** | **I** | **E** | **Y** | **V** | **V** | **Z** | **Y** | **P** | **P** | **H** | **Y** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **5** | **8** | **4** | **24** | **21** | **21** | **25** | **24** | **15** | **15** | **7** | **24** |
| **k** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** |
|  | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** |
| **(C - k) mod N** | **3** | **0** | **11** | **0** | **19** | **13** | **6** | **0** | **13** | **7** | **14** | **0** |
| **P** | **D** | **A** | **L** | **A** | **T** | **N** | **G** | **A** | **N** | **H** | **O** | **A** |

**Kết quả giải mã: P = DA LAT NGAN HOA**

| 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 = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere**

**với C = VPTLJXAMEIGRJW**

| **C** | **V** | **P** | **T** | **L** | **J** | **X** | **A** | **M** | **E** | **I** | **G** | **R** | **J** | **W** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **21** | **15** | **19** | **11** | **9** | **23** | **0** | **12** | **4** | **8** | **6** | **17** | **9** | **22** |
| **k** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** |
|  | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** |
| **(C - k) mod N** | **19** | **7** | **0** | **13** | **7** | **15** | **7** | **14** | **2** | **0** | **13** | **19** | **7** | **14** |
| **P** | **T** | **H** | **A** | **N** | **H** | **P** | **H** | **O** | **C** | **A** | **N** | **T** | **H** | **O** |

**Kết quả giải mã: P =THANH PHO CAN THO**

| 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 = CITY, N = 26, giải mã văn bản, dùng thuật mã Vigenere**

**với C = VPTLJXAMJWTNJCHLILH**

| **C** | **V** | **P** | **T** | **L** | **J** | **X** | **A** | **M** | **J** | **W** | **T** | **N** | **J** | **C** | **H** | **L** | **I** | **L** | **H** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **21** | **15** | **19** | **11** | **9** | **23** | **0** | **12** | **9** | **22** | **19** | **13** | **9** | **2** | **7** | **11** | **8** | **11** | **7** |
| **k** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** | **Y** | **C** | **I** | **T** |
|  | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** | **19** | **24** | **2** | **8** | **19** |
| **(C - k) mod N** | **19** | **7** | **0** | **13** | **7** | **15** | **7** | **14** | **7** | **14** | **0** | **15** | **7** | **20** | **14** | **13** | **6** | **3** | **14** |
| **P** | **T** | **H** | **A** | **N** | **H** | **P** | **H** | **O** | **H** | **O** | **A** | **P** | **H** | **U** | **O** | **N** | **G** | **D** | **O** |

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

| **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** |

**•5. Cho k = MONARCHY, N = 26, mã hóa văn bản, dùng thuật mã Playfair:**

**P = ANTOANBAOMATTHONGTIN**

| **P =** | **A** | **N** | **T** | **O** | **A** | **N** | **B** | **A** | **O** | **M** | **A** | **T** | **T** | **H** | **O** | **N** | **G** | **T** | **I** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **C =** | **R** | **A** | **P** | **R** | **R** | **A** | **I** | **B** | **N** | **O** | **R** | **S** | **P** | **D** | **N** | **A** | **K** | **Q** | **G** | **A** |

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

| **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** |

**•6. Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair:**

**C = FDNRSREBBFOYEFPRRA**

| **C =** | **F** | **D** | **N** | **R** | **S** | **R** | **E** | **B** | **B** | **F** | **O** | **Y** | **E** | **F** | **P** | **R** | **R** | **A** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P =** | **K** | **H** | **O** | **A** | **T** | **A** | **I** | **C** | **H** | **I** | **N** | **H** | **K** | **E** | **T** | **O** | **A** | **N** |

**Kết quả giải mã: P = KHOA TAI CHINH KE TOAN**

| **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** |

**•7. Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair:**

**C = FDNRYQNRGAEWSKOYMH**

| **C =** | **F** | **D** | **N** | **R** | **Y** | **Q** | **N** | **R** | **G** | **A** | **E** | **W** | **S** | **K** | **O** | **Y** | **M** | **H** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P =** | **K** | **H** | **O** | **A** | **N** | **G** | **O** | **A** | **I** | **N** | **G** | **U** | **T** | **I** | **N** | **H** | **O** | **C** |

**Kết quả giải mã: P = KHOA NGOAI NGU TIN HOC**

| **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** |

**•8. Cho k = MONARCHY, N = 26, giải mã văn bản, dùng thuật mã Playfair:**

**C = FDNRABBCWMKYRACZYQ**

| **C =** | **F** | **D** | **N** | **R** | **A** | **B** | **B** | **C** | **W** | **M** | **K** | **Y** | **R** | **A** | **C** | **Z** | **Y** | **Q** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P =** | **K** | **H** | **O** | **A** | **X** | **A** | **Y** | **D** | **U** | **N** | **G** | **D** | **A** | **N** | **D** | **U** | **N** | **G** |

**Kết quả giải mã: P = KHOA XAY DUNG DAN DUNG**

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

**•9. Cho k = KEY, N = 26, giải mã văn bản, dùng thuật mã Playfair:**

**C = BCNBAJOZDVXKOMKFJONA (Đề Sai)**

**C = BCNBCPOGQBXEPVGSMEHISN**

| **C =** | **B** | **C** | **N** | **B** | **C** | **P** | **O** | **G** | **Q** | **B** | **X** | **E** | **P** | **V** | **G** | **S** | **M** | **E** | **H** | **I** | **S** | **N** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P =** | **K** | **H** | **O** | **A** | **K** | **I** | **N** | **H** | **T** | **E** | **V** | **A** | **Q** | **U** | **A** | **N** | **L** | **Y** | **C** | **O** | **N** | **G** |

**Kết quả giải mã: P = KHOA KINH TE VA QUAN LY CONG**

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

**•10. Cho k = KEY, N = 26, giải mã văn bản, dùng thuật mã Playfair:**

**C = SNGSCFJONSYNBGJH**

| **C =** | **S** | **N** | **G** | **S** | **C** | **F** | **J** | **O** | **N** | **S** | **Y** | **N** | **B** | **G** | **J** | **H** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P =** | **N** | **G** | **A** | **N** | **H** | **D** | **O** | **N** | **G** | **N** | **A** | **M** | **A** | **H** | **O** | **C** |

**Kết quả giải mã: P = NGANH DONG NAM A HOC**