**AN TOÀN HỆ THỐNG THÔNG TIN**

**Nhóm 2**

**Thành viên nhóm:** + Trần Thanh Hiệp – 2151050469

+ Bùi Thị Ngân – 2151050271

+ Lê Trí Cường – 2151053007

+ Lê Trung Hiếu – 2151050128

+ Nguyễn Song Hậu – 2151050123

+ Nguyễn Văn Cảnh – 2151053005

+ Nguyễn Hữu Toàn – 2151050462

+ Nguyễn Y Khoa – 2151500202

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

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

**với C = CETUTUFYPFGTIYI**

Văn bản mã được chuyển thành dãy số:

[2, 4, 19, 20, 19, 20, 5, 24, 15, 5, 6, 19, 8, 24, 8]

Nghịch đảo của 11 theo mod của 26 là 19

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

D(x) = a-1(x-b) mod 26 = 19(x – 6) mod 26

Ta được dãy số:

[2, 14, 13, 6, 13, 6, 7, 4, 15, 7, 0, 13, 12, 4, 12]

Ta được bãn rõ CONGNGHEPHANMEM

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

**với  P = CONGNGHETHONGTIN**

Văn bản gốc được chuyển thành dãy số:

[2, 14, 13, 6, 13, 6, 7, 4, 19, 7, 14, 13, 6, 19, 8, 13]

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

E(x) = (ax+b) mod 26 = (17x+12) mod 26

Ta được dãy số:

[20, 16, 25, 10, 25, 10, 1, 2, 23, 1, 16, 25, 10, 23, 18, 25]

Vậy ta được bãn mã: uqzkzkbcxbqzkxsz

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

**với   P = TRUONGDAIHOCMO**

Văn bản gốc được chuyển thành dãy số:

[19, 17, 20, 14, 13, 6, 3, 0, 8, 7, 14, 2, 12, 14]

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

E(x) = (ax+b) mod 26 = (21x+17) mod 26

Ta được dãy số:

[0,10,21,25,,4,13,2,17,3,8,25,7,9,25]

Vậy ta được bãn mã: AKVZENCRDIZHJZ

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

**với C= APWPDGJSFDQW**

Văn bản mã được chuyển thành dãy số:

[0, 15, 22, 15, 3, 6, 9, 18, 5, 3, 16, 22]

Nghịch đảo của 25 theo modulo 26 là 25

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

D(x) = a-1(x-b) mod 26 = 25(x - 29) mod 26

Ta được dãy số

[3, 14, 7, 14, 0, 23 ,20 ,11 ,24 ,0 ,13 ,7]

Vậy ta được bãn mã: DOHOAXYLYANH

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

**với C = WEYEBIPAGI**

Văn bản mã được chuyển thành dãy số:

[22, 4, 24, 4, 1, 8, 15, 0, 6, 8]

Nghịch đảo của 31 theo modulo 26 là 21

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

D(x) = a-1(x-b) mod 26 = 21(x-12) mod 26

Ta được dãy số:

[2,14,18,14,3,20,11,8,4,20]

Ta được bãn rõ COSODULIEU

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

**với P = MANCHESTERUNITED**

Văn bản gốc được chuyển thành dãy số:

[12, 0, 13, 2, 7, 4, 18, 19, 4, 17, 20, 13, 8, 19, 4, 3]

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

E(x) = (ax+b) mod 26 = (31x+24) mod 26

Ta được dãy số:

[6 ,24, 11, 8, 7, 18, 10, 15, 18, 5, 20, 11, 12, 15, 18, 13]

Vậy ta được bãn mã: GYLIHSKPSFULMPSN

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

**C = DYOSFLGULMIHXI**

Văn bản mã được chuyển thành dãy số:

[3, 24, 14, 18, 5, 11, 6, 20, 11, 12, 8, 7, 23, 8]

Nghịch đảo của 31 theo mod của 26 là 21

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

D(x) = a-1(x-b) mod 26 = 21(x-24) mod 26

Ta được dãy số:

[1, 0, 24, 4, 17, 13, 12, 20, 13, 8, 2, 7, 5, 2]

Ta được bãn rõ BAYERNMUNICHFC

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

**C =      ERJSTLNZRC JCMTYJENJ**

Văn bản mã được chuyển thành dãy số:

[4, 17, 9, 18, 19, 11, 13, 25, 17, 2, 9, 2, 12, 19, 24, 9, 4, 13, 9]

Nghịch đảo của 31 theo mod của 26 là 7

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

D(x) = a-1(x-b) mod 26 = 7(x – 35) mod 26

Ta được dãy số:

[17, 4, 0, 11, 18, 14, 2, 8, 4, 3, 0, 3, 21, 18, 1, 0,17, 2,0]

Ta được bãn rõ REALSOCIEDADVSBARCA

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

**C =     OD IOPXFCJVCJXFDOCPVO**

Văn bản mã được chuyển thành dãy số:

[ 14, 3, 8, 14, 15, 23, 52, 9,21 ,2, 9, 23, 5, 3, 14, 2, 15, 21, 14]

Nghịch đảo của 53 theo mod của 26 là 1

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

D(x) = a-1(x-b) mod 26 = (x – 21) mod 26

Ta được dãy số:

[19,8,13,19,20,2, 10, 7,14, 0, 7,14, 2, 10,8, 19,7,20,0,19]

Ta được bãn rõ TINTUCKHOAHOCKITHUAT

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

**C =      OCPJIBICVPGTOJCJIB**

Bản mã C được đổi thành dãy số:

[14, 2, 15, 9, 8, 1, 8, 2, 21, 15, 6, 19, 14, 9, 2, 9, 8, 1]

Nghịch đảo modulo 26 của 53 là 1

Với từng số x trong dãy số trên, áp dụng hàm mã hoá

D(x) = a-1(x-b) mod 26 = (x-47) mod 26

Ta được dãy số:

[19, 7, 20, 14, 13, 6, 13, 7, 0, 20, 11, 24, 19, 14, 7, 14, 13, 6]

Vậy ta được bãn mã: THUONGNHAULYTOHONG