Câu 1 (3 đ):

a. Passive Attack (tấn công bị động) lấy thông tin từ hệ thống nhưng *không làm ảnh hưởng đến tài nguyên của hệ thống*. Active Attack (tấn công chủ động) *làm thay đổi tài nguyên* hoặc *làm ảnh hưởng đến hoạt động của hệ thống*. (1đ)

b1. Passive Attack gồm các hình thức: (1đ)

- **Nghe lén (release of message contents)**: các cuộc điện thoại, email hoặc tập tin được truyền trên mạng có thể chứa các thông tin nhạy cảm, bí mật mà kẻ tấn công sẽ tìm mọi cách để đọc được.
- **Phân tích lưu lượng đường truyền (traffic analysis)**: theo dõi mẫu thức, tần số và độ dài của các thông điệp để dự đoán tính chất của các thông tin khi không thể đọc được nội dung.

b2. Active Attack gồm các hình thức: (1đ)

- **Giả mạo (Masquerade)**: kẻ tấn công có thể mạo danh một người nào đó để thực hiện một thao tác trên hệ thống hoặc gửi thông điệp đến người khác.
- **Phát lại (Replay)**: kẻ tấn công đọc được nội dung thông điệp từ nơi gửi (người, hệ thống) và sau đó gửi lại thông điệp này đến nơi nhận (người, hệ thống) để thực hiện một hành vi trái phép.
- **Chỉnh sửa nội dung thông điệp**: thông điệp gửi đi bị kẻ tấn công thay đổi, chỉnh sửa để thực hiện các hành vi trái phép.
- **Tấn công từ chối dịch vụ (Denial of Service)**: làm gián đoạn hoặc tê liệt hệ thống dẫn đến người dùng không thể sử dụng hay truy cập tài nguyên của hệ thống.

Câu 2 (4đ): a,b,c,d: Mỗi mục 1 đ

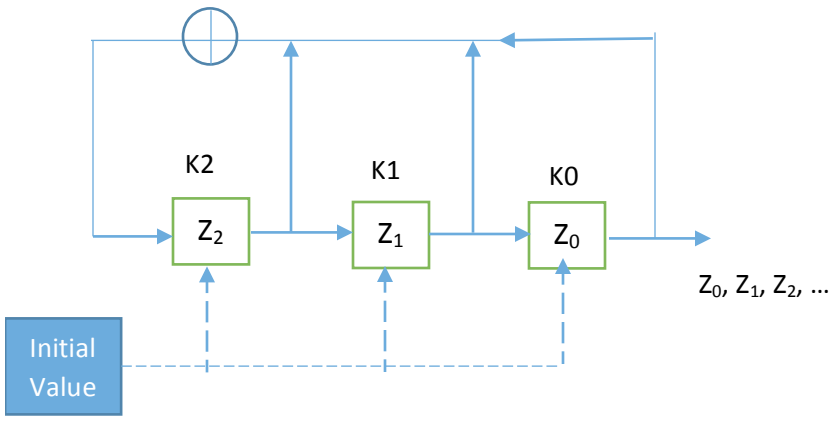
a. $A = (3, 1 + x + x^2 + x^3)$, $[z_0, z_1, z_2] = [1, 0, 1]$

$C_0 = 1, C_1 = 1, C_2 = 1$

K2	K1	K0
1	0	1
0	1	0
1	0	1

Dòng khóa thu được: (10).

Chu kỳ: 2



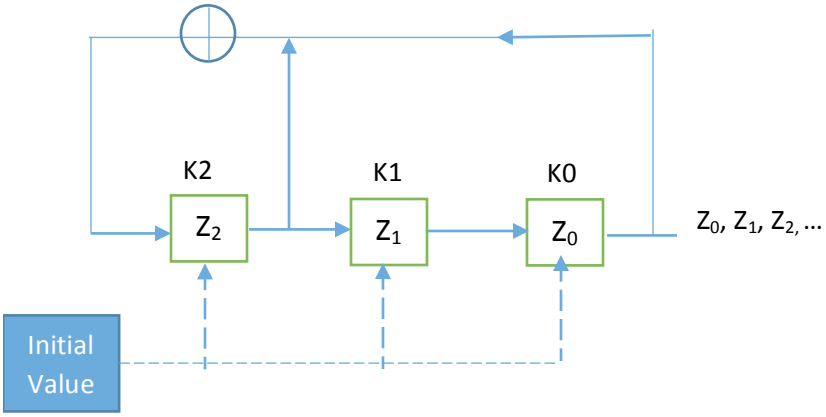
b. $B = (3, 1 + x^2 + x^3)$, $[z_0, z_1, z_2] = [0, 0, 1]$

$C_0 = 1, C_1 = 0, C_2 = 1$

K2	K1	K0
1	0	0
1	1	0
1	1	1
0	1	1
1	0	1
0	1	0
0	0	1
1	0	0

Dòng khóa thu được: (0011101)

Chu kỳ: 7



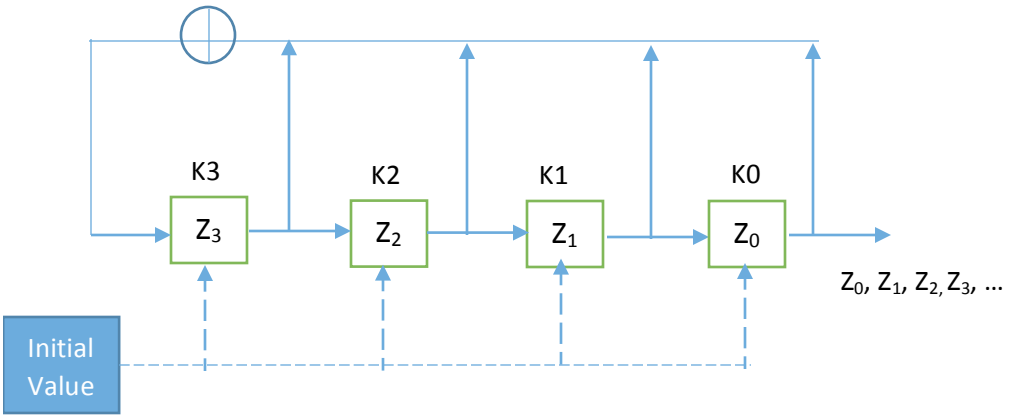
c. $C = (4, 1 + x + x^2 + x^3 + x^4)$, $[z_0, z_1, z_2, z_3] = [1, 0, 1, 0]$

$C_0 = 1, C_1 = 1, C_2 = 1, C_3 = 1$

K3	K2	K1	K0
0	1	0	1
0	0	1	0
1	0	0	1
0	1	0	0
1	0	1	0
0	1	0	1

Dòng khóa thu được: (10100)

Chu kỳ: 5



d. Tính Z_{150}

$Z_n = b_{t(n)-1} + c_{n-t(n)}$ với $t(n) = \sum_{i=0}^{n} a_i$

n = 150, $t(150) = \sum_{i=0}^{150} a_i$ = 151 số, chu kỳ của A là 2, 151/2 = 75 dư 1 → biểu diễn A:

$$\overbrace{(10)}^{75\ lần} 1$$

t(150) = 1 * 75 + 1 = 76

Suy ra $Z_{150} = b_{76-1} + c_{150-76} = b_{75} + c_{74}$

b_{75} là bit thứ 76, chu kỳ của B là 7, 76/7 = 10 dư 6, biểu diễn B:

$$\overbrace{(0011101)}^{10\ lần} 001110$$

Suy ra $b_{75} = 0$ (Hoặc $b_{75} = b_{(75 \bmod 7)} = b_5 = 0$)

c_{74} là bit thứ 75, chu kỳ C là 5, 75/5 = 15, biểu diễn C:

$$\overbrace{(10100)}^{15\ lần}$$

Suy ra $c_{74} = 0$ (Hoặc $c_{74} = c_{(74 \bmod 5)} = c_4 = 0$)

- Vậy $Z_{150} = b_{75} + c_{74} = 0$

Câu 3 (3đ):

Bước 1: TẠO KHÓA (1đ)

N = p×q = 5 × 11 = 55; ϕ(N) = (p-1) × (q-1) = 40; (e, ϕ(N)) = (7,40) = (7,5) = (5,2) = (2,1) = 1

Tính $d = e^{-1} \bmod \phi(N) = 7^{-1} \bmod 40$

y	q	v
-	40	0
-	7	1
5	5	-5
1	2	6
2	1	-17 = 23

Khóa công khai: (7, 55)

Khóa cá nhân: (23, 55)

Bước 2: MÃ HÓA (1đ)

Mã hóa : $C = M^e \bmod N = 36^7 \bmod 55$

$7 = 111_2$

sm	kq	cs
111	1	36
1	1×36 = 36	$36^2 = 1296 = 31$
1	36×31 = 1116 = 16	$31^2 = 961 = 26$
1	16×26 = 416 = 31	-

Bản mã: C=31

Bước 3: GIẢI MÃ (1đ)

Giải mã: $M' = C^d \bmod N = 31^{23} \bmod 55$

$23 = 10111_2$

sm	kq	cs
10111	1	31
1	1×31= 31	31^2= 961= 26
1	26×31= 806= 36	26^2 = 676 = 16
1	16×36= 576= 26	16^2 = 256 = 36
0	-	36^2 = 1296= 31
1	26×31= 806= **36**	

M’ = 26 = M. Quá trình mã hoá và giải mã thành công!