# Báo Cáo: Các Hệ Mật và Sơ Đồ Chữ Ký Số

Lớp: Mật mã và An toàn thông tin ( INT3230E 53)

Giảng viên: GVC.TS Lê Phê Đô

Trần Huy Hoàng

Mã sinh viên: 22028183

Ngày sinh: 21/7/2004

## 1. Giới thiệu

Trong kỷ nguyên số, bảo mật thông tin là một lĩnh vực quan trọng nhằm bảo vệ tính toàn vẹn, tính bảo mật và tính xác thực của dữ liệu. Các hệ mật (hay hệ mã hóa) và sơ đồ chữ ký số là hai trong số các công cụ quan trọng nhất được sử dụng để đảm bảo rằng dữ liệu được bảo vệ trong quá trình truyền tải hoặc lưu trữ, cũng như xác thực được danh tính của người gửi.  
  
- Các hệ mật đóng vai trò mã hóa thông tin, chuyển đổi bản rõ (dữ liệu ban đầu) thành bản mã (dữ liệu đã mã hóa) để chỉ người có khóa bí mật mới có thể giải mã và truy cập thông tin gốc. Các hệ mật được áp dụng rộng rãi trong truyền thông bảo mật, dịch vụ ngân hàng, và các hệ thống yêu cầu bảo mật cao như chính phủ và quân đội.  
  
- Sơ đồ chữ ký số cung cấp phương thức xác thực dữ liệu, cho phép người nhận kiểm tra tính xác thực và tính toàn vẹn của thông tin nhận được. Với chữ ký số, người nhận có thể chắc chắn rằng thông tin đến từ đúng người gửi và chưa bị thay đổi trong quá trình truyền tải

## 2. Hệ mật RSA

Hệ mật RSA (Rivest–Shamir–Adleman) là một trong những hệ mã hóa khóa công khai phổ biến nhất, dựa trên độ khó của bài toán phân tích thành thừa số của các số nguyên lớn.

- Các tham số chính: RSA sử dụng hai số nguyên tố lớn để tạo nên khóa công khai và khóa bí mật.  
- Quá trình mã hóa: Bản rõ được mã hóa bằng khóa công khai của người nhận, và chỉ người nhận với khóa bí mật tương ứng mới có thể giải mã bản mã.  
- Ứng dụng: RSA thường được dùng để mã hóa dữ liệu nhạy cảm và xác thực danh tính trong các giao dịch tài chính.

#### Các bước thực hiện:

1. Chọn hai số nguyên tố lớn p và q.

2. Tính n = p × q và φ(n) = (p-1)(q-1).

3. Chọn số nguyên e sao cho gcd(e, φ(n)) = 1.

4. Tính số d sao cho d × e ≡ 1 (mod φ(n)).

##### Khóa công khai - khóa bí mật:

Khóa công khai: (e, n) và khóa bí mật: d.

##### Quá trình mã hóa và giải mã:

Mã hóa: Với bản rõ m, bản mã là c = m^e mod n.

Giải mã: Với bản mã c, bản rõ là m = c^d mod n.

#### Áp dụng cho bản tin x = 714013621032014136 (kết quả ở dưới là phần tóm tắt với 26 chữ số, về kết quả cụ thể, nhóm em lưu trong folder Hệ mật RSA)

Ta chọn 2 số p và q như sau:

p= 96693629286532733538006296...

q = 33915270318808967406534795...

Tính được

n = 32793905753594611294093113...

phi\_n = 32793905753594611294093...

e = 65537

d = 10166375989071543062118952...

Ta mã hóa x, được ciphertext là: 9011410103665440764683466106298346589300507265907782833298567114569775458888055660711...

Giải mã ngược đoạn mã hóa ta được, sau khi giải mã: 714013621032014136.

Với kết quả như vậy, ta nhận thấy ta đã mã hóa đúng và giải mã thành công!

* Kết quả hệ mật RSA: nhóm chúng em đã thực hiện chạy với số p và q là số có 10000 chữ số (tương đương 33,200 bit) và n = p\* q là số có 20000 chữ số (tương đương 66,400 bit), kết quả ở trên là phần tóm tắt với 26 chữ số, về kết quả cụ thể, nhóm em lưu trong folder Hệ mật RSA

## 3. Hệ mật Elgamal

Elgamal là hệ mã hóa khóa công khai dựa trên độ khó của bài toán tính logarit rời rạc, cung cấp tính bảo mật mạnh mẽ và linh hoạt.

- Các tham số chính: Elgamal sử dụng một số nguyên tố lớn và phần tử sinh để tạo khóa công khai và khóa bí mật.  
- Quá trình mã hóa: Dữ liệu bản rõ được mã hóa bằng khóa công khai, tạo ra bản mã dưới dạng hai phần tử mà chỉ có khóa bí mật mới giải mã được.  
- Ứng dụng: Elgamal thường được dùng trong các hệ thống yêu cầu bảo mật cao và là nền tảng cho nhiều giao thức bảo mật hiện đại.

#### Các bước thực hiện:

##### Chọn tham số

1. Chọn một số nguyên tố lớn p.

2. Chọn phần tử nguyên thuỷ α của p - 1 .

3. Khóa bí mật a bất kỳ thuộc Zp-1 và khóa công khai β = α^a mod p.

##### Khóa công khai và bí mật:

Khóa công khai (p, α, β) và khóa bí mật a

##### Quá trình mã hóa và giải mã:

Mã hóa: Với plaintext m và số ngẫu nhiên k thuộc Zp-1:

y1 = α^k mod p

y2 = m × β^k mod p

Giải mã: m = y2 / (y1^a)^-1 mod p.   
Áp dụng cho bản tin x = 4116012011. (kết quả ở dưới là phần tóm tắt với 26 chữ số, về kết quả cụ thể, nhóm em lưu trong folder Hệ mật Elgamal)

1. Ta chọn

p = 88025135843934728967088739...

a = 74975559236015947629499617...

k = 12886616550801912225611933...

2. Tìm được phần từ nguyên thủy: α = 2

3. Tính β = α^a mod p =23557103042830134200244407...

4. Ciphertext là (y1, y2) với

y1 = 52930915459899296964783954...

y2 = 69024484132312713433298266...

5. Tiến hành giải mã:

m = y2 / (y1^a)^-1 mod p.  
 = 4116012011

Với kết quả như vậy, ta nhận thấy ta đã mã hóa đúng và giải mã thành công!

* Kết quả hệ mật Elgamal: nhóm chúng em đã thực hiện chạy với số p có 2466 chữ số (tương đương 8192 bit), kết quả ở trên là phần tóm tắt với 26 chữ số, về kết quả cụ thể, nhóm em lưu trong folder Hệ mật Elgamal

## 4. Hệ mật Elliptic Curve Cryptography (ECC)

ECC (Mã hóa Đường cong Elliptic) là hệ mật hiện đại, sử dụng toán học đường cong elliptic trên các trường hữu hạn. ECC nổi bật với khả năng cung cấp mức độ bảo mật cao với độ dài khóa ngắn hơn so với RSA và Elgamal.

- Các tham số chính: ECC sử dụng một điểm sinh trên đường cong elliptic và một khóa bí mật để tạo khóa công khai.

y^2 ≡ x^3 + ax + b (mod p)  
  
 với:  
 + a và b là các tham số cố định sao cho phương trình 4a^3 + 27b^2 ≠ 0 (mod p) để tránh các điểm kỳ dị.  
 + p là một số nguyên tố lớn, xác định trường hữu hạn.  
- Quá trình mã hóa: ECC khai thác bài toán logarithm rời rạc trên đường cong elliptic (Elliptic Curve Discrete Logarithm Problem - ECDLP), trong đó, cho trước hai điểm P và Q = kP trên đường cong elliptic, rất khó để tìm k, đặc biệt khi k và p rất lớn.  
- Ứng dụng: ECC phù hợp cho các thiết bị hạn chế về tài nguyên như điện thoại di động và thiết bị IoT, nhờ khả năng cung cấp bảo mật với khóa ngắn hơn.

#### Các bước thực hiện:

##### Khóa công khai và bí mật:

##### Tạo Khóa: - Khóa riêng: Một số ngẫu nhiên d chọn từ khoảng [1, p-1]. - Khóa công khai: Tính toán bằng cách nhân điểm sinh G với khóa riêng d để có Q = dG.

##### Quá trình mã hóa và giải mã:

Mã hóa:  
- Biểu diễn thông điệp M dưới dạng một điểm trên đường cong elliptic. (Dùng hàm ánh xạ).  
- Chọn số ngẫu nhiên k từ khoảng [1, p-1].  
- Tính hai điểm:  
 M1 = kG, với k là một số ngẫu nhiên.  
 M2 = M + kQ, trong đó M là điểm ánh xạ từ thông điệp.  
- Cặp điểm (M1, M2) là thông điệp mã hóa.  
  
Giải mã:  
- Người nhận sử dụng khóa riêng d để tính S = dM1.  
- Sau đó, tính M bằng M = M2 - S, vì M2 = M + kQ = M + kdG.

#### Áp dụng cho bản tin x = 20160091143476977738780

##### Bản tin được ánh xạ sang đường cong eliptic:

x: 20160091143476977738783

y: 6670436481353467126837250659607422281444328801365926386428246089962752257520925908803558903205666042073062562303259890117872954787420769671590696876042515

##### Ta chọn a, b, p sao cho tạo thành đường cong có nhóm cyclic tức là số điểm nằm thuộc đường cong là số nguyên tố

p:8948962207650232551656602815159153422162609644098354511344597187200057010413552439917934304191956942765446530386427345937963894309923928536070534607816947

a:6294860557973063227666421306476379324074715770622746227136910445450301914281276098027990968407983962691151853678563877834221834027439718238065725844264138

b:3245789008328967059274849584342077916531909009637501918328323668736179176583263496463525128488282611559800773506973771797764811498834995234341530862286627

Ta được đường cong eliptic: y^2 = x^3 + 6294860557973063227666421306476379324074715770622746227136910445450301914281276098027990968407983962691151853678563877834221834027439718238065725844264138x + 3245789008328967059274849584342077916531909009637501918328323668736179176583263496463525128488282611559800773506973771797764811498834995234341530862286627 mod (8948962207650232551656602815159153422162609644098354511344597187200057010413552439917934304191956942765446530386427345937963894309923928536070534607816947)

Ta chọn điểm sinh là:

Điểm sinh G

x: 6792059140424575174435640431269195087843153390102521881468023012732047482579853077545647446272866794936371522410774532686582484617946013928874296844351522

y: 6592244555240112873324748381429610341312712940326266331327445066687010545415256461097707483288650216992613090185042957716318301180159234788504307628509330

##### Từ đó, ta chọn khóa công khai và khóa bí mật

Khóa riêng: 8235723350881222093275278161838509844561292848363058075428232681859893292265611988187732481134380074435078658564655354621689131289716497074207806418384658

Khóa công khai:

x = 7765237731104069819393091269824391877721693952308756206082178375757111038420087697932087346453372091208393268709478685343433417648690512854917789145303513

y = 2858482357119196410171423975608726121805302179166375804806692192537036431875895504059426417235885273834160639330351796298644082648393840861698514581379541

##### Ta tiến hành mã hóa và giải mã:

Thông điệp đã mã hóa (M1, M2):

M1: 7151866082890293551196059345546782727330273833949397171028355225958565902127987011217862957291303275578534647238485405497560236905376288605186881176179041 4582737527431891557449423919625002474013539251498675644511904107611971212126164644901745183008092300245807619302518539668332781357669126558646812731927135

M2: 6325632987871495696145297497346092425054485149988590658939867283848481138365144598844751675651496735211745558928151790023839541746482876343557765878555471 1900216392267102421903544224668844668313002611819474327732076417443620652464412864794116277253161865876245182922788223801841049089104581216443495663531414

Thông điệp giải mã dưới dạng điểm:

x: 20160091143476977738783

y: 6670436481353467126837250659607422281444328801365926386428246089962752257520925908803558903205666042073062562303259890117872954787420769671590696876042515

Với kết quả như vậy, ta nhận thấy ta đã mã hóa đúng và giải mã thành công!

* Kết quả hệ mật ECC: nhóm chúng em đã thực hiện chạy với số p có 154 chữ số (tương đương 512 bit), a và b có 154 chữ số (tương đương 512 bit)

## 5. Sơ đồ chữ ký số RSA

Sơ đồ chữ ký số RSA sử dụng chính hệ mật RSA để ký và xác thực thông tin. Người gửi tạo chữ ký số bằng khóa bí mật của mình và người nhận có thể xác thực chữ ký bằng khóa công khai.

- Cách hoạt động: Chữ ký số được tạo bằng cách mã hóa một băm của thông điệp với khóa bí mật. Người nhận sẽ giải mã chữ ký bằng khóa công khai để kiểm tra tính toàn vẹn của thông điệp.

#### Các bước thực hiện:

Chọn tham số

1. Chọn hai số nguyên tố lớn p và q.

2. Tính n = p × q và φ(n) = (p-1)(q-1).

3. Chọn số nguyên e sao cho gcd(e, φ(n)) = 1.

4. Tính số d sao cho d × e ≡ 1 (mod φ(n)).

##### Khóa công khai - khóa bí mật:

Khóa công khai: (e, n) và khóa bí mật: d.

##### Quá trình ký và xác minh

Ta băm thông tin về dạng h(x) và bắt đầu tạo chữ ký và xác thực

Tạo chữ ký: s = h(x)^d mod n.

Xác minh chữ ký: Kiểm tra h(x) ≡ s^e mod n.

#### Áp dụng cho bản tin h(x) = 714013621032014136 (kết quả ở dưới là phần tóm tắt với 26 chữ số, về kết quả cụ thể gồm 10000 chữ số, nhóm em lưu trong folder Hệ sơ đồ chữ ký RSA)

1. Ta chọn 2 số p và q như sau:

p= 96693629286532733538006296...

q = 33915270318808967406534795...

2. Tính được

n = 32793905753594611294093113...

phi\_n = 32793905753594611294093...

e = 65537

d = 10166375989071543062118952...

3. Ta tạo chữ ký và nhận được chữ ký là: 9011410103665440764683466106298346589300507265907782833298567114569775458888055660711...

4. Sau khi xác minh, ta nhận được: h(x) = 9011410103665440764683466106298346589300507265907782833298567114569775458888055660711... ^ e mod n. = 714013621032014136

Ta thấy chữ ký hợp lệ!

* Kết quả sơ đồ chữ ký RSA: nhóm chúng em đã thực hiện chạy với số p và q là số có 10000 chữ số (tương đương 33,200 bit) và n = p\* q là số có 20000 chữ số (tương đương 66,400 bit), kết quả ở trên là phần tóm tắt với 26 chữ số, về kết quả cụ thể 10000 chữ số, nhóm em lưu trong folder Hệ sơ đồ chữ ký RSA

## 6. Sơ đồ chữ ký số Elgamal

Chữ ký số Elgamal cung cấp một cách xác thực thông tin dựa trên hệ mật Elgamal, với tính an toàn dựa trên logarit rời rạc.

- Cách hoạt động: Chữ ký được tạo dựa trên các tham số ngẫu nhiên và khóa bí mật của người gửi. Người nhận kiểm tra chữ ký bằng cách sử dụng khóa công khai để đảm bảo rằng thông điệp chưa bị thay đổi và đến từ đúng người gửi.

#### Các bước thực hiện:

##### Chọn tham số

1. Chọn một số nguyên tố lớn p.

2. Chọn phần tử nguyên thuỷ α của p - 1 .

3. Khóa bí mật a bất kỳ thuộc Zp-1 và khóa công khai β = α^a mod p.

##### Khóa công khai và bí mật:

Khóa công khai (p, α, β) và khóa bí mật a

##### Quá trình ký và xác minh:

Ký: Với plaintext m và số ngẫu nhiên k thuộc Zp-1:

γ = α^k mod p.  
 σ = ((h(x) - a \* γ) \* k^-1 mod (p - 1)

Xác minh:

- Tính giá trị β^γ \* γ^σ mod p.  
- Tính giá trị α^{h(x)} mod p.  
 - So sánh 2 giá trị trên để xác minh tính hợp lệ của chữ ký.

Áp dụng cho bản tin h(x) = 197818818122418861301920174. (kết quả ở dưới là phần tóm tắt với 26 chữ số, về kết quả cụ thể, nhóm em lưu trong folder Sơ đồ chữ ký Elgamal)

1. Ta chọn

p = 88025135843934728967088739...

a = 73701470733256490835898502...

k = 38590902108221603809382278...

2. Tìm được phần từ nguyên thủy: α = 2

3. Tính β = α^a mod p =60665710273234925427190046...

4. Ký với với

γ = 66142054047873352608853366...

σ = 45176533212310392235728194...

5.Xác minh chữ ký:

β^γ \* γ^σ mod p = α^{h(x)} mod p  
Ta thấy chữ ký hợp lệ!

Với kết quả như vậy, ta nhận thấy ta đã mã hóa đúng và giải mã thành công!

* Kết quả sơ đồ chữ ký Elgamal: nhóm chúng em đã thực hiện chạy với số p có 2466 chữ số (tương đương 8192 bit), kết quả ở trên là phần tóm tắt với 26 chữ số, về kết quả cụ thể, nhóm em lưu trong folder Sơ đồ chữ ký Elgamal

## 7. Sơ đồ chữ ký số ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm) là một thuật toán chữ ký số dựa trên đường cong elliptic, được sử dụng để tạo và xác minh chữ ký số với mức độ bảo mật cao và kích thước khóa nhỏ hơn so với các phương pháp truyền thống như RSA. Trong ECDSA, chữ ký số được tạo bằng khóa riêng và có thể xác minh tính hợp lệ bằng khóa công khai tương ứng.

- Cách hoạt động: Chữ ký ECDSA bao gồm hai giá trị được tạo từ thông điệp và khóa bí mật của người gửi. Người nhận sử dụng khóa công khai để kiểm tra tính hợp lệ của chữ ký và đảm bảo tính xác thực của thông điệp.

Một đường cong elliptic trên trường hữu hạn được định nghĩa bởi phương trình:  
 y^2 ≡ x^3 + ax + b (mod p)  
với các tham số:  
- `p`: Số nguyên tố xác định trường hữu hạn.  
- `A` và `B`: Các tham số của đường cong elliptic.  
- `G`: Điểm sinh trên đường cong, được dùng làm điểm cơ sở để sinh khóa công khai.  
- `n`: Bậc của điểm sinh G (số lượng điểm trên đường cong khi bắt đầu từ G và thực hiện các phép cộng điểm).

#### Các bước thực hiện:

##### Khóa công khai và bí mật:

- Chọn khóa riêng `d`: một số ngẫu nhiên trong khoảng [1, n-1].  
- Tính khóa công khai `Q`: bằng phép nhân vô hướng giữa `d` và điểm sinh `G`, theo công thức:  
 Q = d \* G  
- Khóa công khai `Q` là một điểm trên đường cong elliptic, có thể chia sẻ công khai, trong khi khóa riêng `d` phải được giữ bí mật.

##### Tạo Chữ Ký ECDSA

Để tạo chữ ký số ECDSA cho một thông điệp, các bước sau được thực hiện:  
- Bước 1: Chọn một số ngẫu nhiên k trong khoảng [1, n-1].  
- Bước 2: Tính điểm kG trên đường cong, và lấy tọa độ x của kG để tính r:  
 r = x\_kG mod n  
- Nếu r = 0, chọn lại k.  
- Bước 3: Tính s theo công thức:  
 s = k^(-1) \* (message + d \* r) mod n  
 với k^(-1) là nghịch đảo modular của `k` modulo `n`.  
- Nếu `s = 0`, chọn lại k và tính lại r và s.  
- Chữ ký cuối cùng là cặp (r, s).

##### 5. Xác Minh Chữ Ký ECDSA

Để xác minh chữ ký (r, s) với một thông điệp, các bước sau được thực hiện:  
- Bước 1: Kiểm tra tính hợp lệ của r và s: chúng phải thỏa mãn 0 < r < n và 0 < s < n.  
- Bước 2: Tính s\_inv, nghịch đảo modular của s modulo n.  
- Bước 3: Tính hai giá trị u1 và u2:  
 u1 = message \* s\_inv mod n  
 u2 = r \* s\_inv mod n  
- Bước 4: Tính hai điểm u1 \* G và u2 \* Q trên đường cong elliptic, sau đó cộng chúng lại để thu được một điểm:  
 Point\_sum = u1 \* G + u2 \* Q  
- Bước 5: Kiểm tra tọa độ x của `Point\_sum`. Nếu x\_Point\_sum mod n = r mod n, chữ ký hợp lệ; nếu không, chữ ký không hợp lệ.

Áp dụng cho bản tin h(x) = ***20160091143476977738780***

##### Ta chọn a, b, p sao cho tạo thành đường cong có nhóm cyclic tức là số điểm nằm thuộc đường cong là số nguyên tố.

a: 6294860557973063227666421306476379324074715770622746227136910445450301914281276098027990968407983962691151853678563877834221834027439718238065725844264138

b: 3245789008328967059274849584342077916531909009637501918328323668736179176583263496463525128488282611559800773506973771797764811498834995234341530862286627

p: 8948962207650232551656602815159153422162609644098354511344597187200057010413552439917934304191956942765446530386427345937963894309923928536070534607816947

##### Ta được đường cong eliptic

y^2 = x^3 + 6294860557973063227666421306476379324074715770622746227136910445450301914281276098027990968407983962691151853678563877834221834027439718238065725844264138x + 3245789008328967059274849584342077916531909009637501918328323668736179176583263496463525128488282611559800773506973771797764811498834995234341530862286627 (mod 8948962207650232551656602815159153422162609644098354511344597187200057010413552439917934304191956942765446530386427345937963894309923928536070534607816947)

##### Ta chọn điểm sinh:

Điểm sinh (G):

x: 6792059140424575174435640431269195087843153390102521881468023012732047482579853077545647446272866794936371522410774532686582484617946013928874296844351522

y: 6592244555240112873324748381429610341312712940326266331327445066687010545415256461097707483288650216992613090185042957716318301180159234788504307628509330

Từ đường cong trên, ta tính tổng số điểm là: 8948962207650232551656602815159153422162609644098354511344597187200057010413418528378981730643524959857451398370029280583094215613882043973354392115544169

* Kiểm tra ta thấy đây là số nguyên tố, nghĩa là đường cong là đường cong tạo thành nhóm cyclic.

##### Và điểm đối của điểm sinh là:

x: 6792059140424575174435640431269195087843153390102521881468023012732047482579853077545647446272866794936371522410774532686582484617946013928874296844351522

y: 2356717652410119678331854433729543080849896703772088180017152120513046464998295978820226820903306725772833440201384388221645593129764693747566226979307617

##### Từ đó, ta có khóa công khai và khóa bí mật:

Private key: 3873267397104332032956644312503270385793777529171630749672560824551207173383401564823757019893355160447429549392746733090753875483756524208034197189138879

Public key: (7332158739232903274049308502554523980971843190319086355551994463041556808983144355140525980630601384093429749418205392157544198733170552127770244509850210, 5071538035200455719324862744811408091645006478983803837982042719006632904702460526288080375236261202474280607518538636872032933855469939475353265453850581)

##### Từ đó ta tìm ra chữ ký

Signature (r, s): (7332158739232903274049308502554523980971843190319086355551994463041556808983144355140525980630601384093429749418205392157544198733170552127770244509850210, 8429645242587301840052334676009986211327154633418642393017861840220884473157581157923345305329145563272100723278800922117482141759304418706186767869193399)

Xác minh chữ ký, ta thấy chữ ký là hợp lệ !!

* Kết quả sơ đồ chữ ký ECDSA: nhóm chúng em đã thực hiện chạy với số p có 154 chữ số (tương đương 512 bit), a và b có 154 chữ số (tương đương 512 bit)

## 8. Kết luận

Các hệ mật và sơ đồ chữ ký số như RSA, Elgamal, ECC và ECDSA đều cung cấp các phương pháp bảo mật cần thiết cho nhiều ứng dụng thực tế, từ giao dịch tài chính đến bảo mật trong các thiết bị thông minh. Việc lựa chọn phương pháp phù hợp tùy thuộc vào yêu cầu về bảo mật, tốc độ và tài nguyên của hệ thống ứng dụng.