Cấu trúc đề thi giữa kỳ Nhập môn An Toàn Thông Tin

Mỗi bài 01 điểm. Làm bài luôn vào đề.

Yêu cầu: Viết sáng sủa và ngắn gọn; Không nháp vào bài thi.

Bài 1. Thuật toán Euclid mở rộng.

Bài 2. Thuật toán tính luỹ thừa nhanh.

Bài 3. Hàm logarit rời rạc và hàm Diffie-Hellman.

Bài 4. Tính toán trên trường hữu hạn.

Bài 5. Đường cong Elliptic và giao thức Diffie-Hellman.

Bài 6. Giao thức Diffie-Hellman.

Bài 7. Hệ mật RSA.

Bài 8. Tấn công ở giữa (meet-in-the-middle).

Bài 9. One-time-pad hoặc CTR-mode hoặc CBC-mode.

Bài 10. MAC.

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Họ tên SV: ..... MSSV: .....

Học phần: **Nhập môn An Toàn Thông Tin** ..... Mã HP: .....

Bài thi [ ] giữa kỳ [X] cuối kỳ ..... Ngày thi:.....

Số thứ tự

Điểm của bài thi	Chữ ký của (các) cán bộ chấm thi	Chữ ký của cán bộ coi thi

Đề thi mẫu giữa kỳ Nhập môn An Toàn Thông Tin
Thời gian 90 phút. Không sử dụng tài liệu.

1. Hãy dùng thuật toán Euclid mở rộng để tính $28^{-1} \mod 75$. Hãy mô tả chi tiết từng bước trong quá trình tính toán.

2. Hãy dùng thuật toán tính luỹ thừa nhanh để tính $9726^{3533} \mod 11413$.

3. Xét nhóm $\mathbb{Z}_{19}^*$ với 3 là một phần tử sinh. Hãy tính logarit rời rạc $\mathrm{Dlog}_3(15)$ trong nhóm này; và dùng nó để tính giá trị của hàm Diffie-Hellman $\mathrm{DH}_3(7, 15)$.

4. Tính đa thức

$$(x^4 + x + 1)/(x^7 + x^6 + x^3 + x^2),$$

trong $GF(2^8)$ với đa thức bất khả quy là $P(x) = x^8 + x^4 + x^3 + x + 1$ (đa thức AES).

5. Xét đường cong Elliptic

$$E: \qquad y^2 = x^3 + 2x + 2 \mod 17$$

và điểm $P = (13, 7)$. Alice và Bob sẽ thiết lập khoá chia sẻ dùng giao thức Diffie-Hellman trên đường cong E. Cụ thể, Alice sẽ thực hiện:

- Chọn giá trị $a = 4$ và gửi điểm aP cho Bob;
- Nhận được điểm $bP = (6, 3)$ từ Bob.

Hãy tính khoá chia sẻ abP giữa Alice và Bob.

6. Giả sử có $n+1$ bên, gọi là $B, A_1, \ldots, A_n$, muốn có một khóa chung cho cả nhóm. Họ muốn có một giao thức sao cho mọi người đều có chung một khóa chia sẻ, nhưng kẻ nghe lén dù thấy được toàn bộ quá trình trao đổi vẫn không tính được khoá chia sẻ này.

Các bên thống nhất một nhóm G có cấp nguyên tố q với phần tử sinh g và dùng giao thức sau đây :

- Mỗi bên A_i chọn một số ngẫu nhiên a_i thuộc $\{1, \ldots, q\}$ và gửi cho Bên B giá trị $X_i \leftarrow g^{a_i}$.
- Bên B sinh một số ngẫu nhiên b thuộc $\{1, \ldots, q\}$ và trả lại bên A_i thông điệp $Y_i \leftarrow X_i^b$.

Khóa chia sẻ của nhóm là g^b. Rõ ràng Bên B có thể tính được khóa này. Các bên A_i tính khóa này như thế nào ? Hãy giải thích ngắn gọn.

7. Nhắc lại rằng hoán vị cửa sập RSA được định nghĩa trong nhóm $\mathbb{Z}_N^*$ với N là tích của hai số nguyên tố lớn. Khóa công khai là (N, e) và khóa bí mật là (N, d) trong đó d là nghịch đảo của e trong $\mathbb{Z}_{\varphi(N)}^*$.

Giả sử trong thuật toán RSA, thay vì dùng hợp số N bạn lại dùng số nguyên tố p. Hãy chỉ ra rằng trong trường hợp này mọi người đều có thể tính hoặc không tính được khóa bí mật (N, d) từ khóa công khai (N, e) bằng cách tính dưới đây. Hãy giải thích ngắn gọn.

1. $d = -e \pmod{p}$.

2. $d = e^2 \pmod{p}$.

3. $d = e^{-1} \pmod{p}$.

4. $d = e^{-1} \pmod{p-1}$.

8. Xét hệ mã khối $\mathscr{E} = (E, D)$ an toàn trên không gian khoá $\mathscr{K}$. Ta xây dựng hệ $4\mathscr{E}$ từ $\mathscr{E}$ bằng cách lặp lại việc mã hoá bốn lần dùng bốn khoá khác nhau:

$$E_4(\,(k_1, k_2, k_3, k_4)\,, m) = E(k_4,\ E(k_3,\ E(k_2,\ E(k_1,\ m)))).$$

Hãy mô tả cách tấn công ở giữa (meet-in-the-middle) để khôi phục khoá bí mật của $4\mathscr{E}$ trong thời gian $|\mathscr{K}|^2$ và với bộ nhớ $|\mathscr{K}|^2$.

9. An chuyển tiền cho Bình qua một hệ thống ngân hàng. Số tiền được biểu diễn bằng một số nguyên 8-bit. An mã hóa số tiền dùng CTR-mode dựa trên một hệ mã khối với kích thước khối là 8-bit! Bình biết số tiền An chuyển cho mình chỉ là 16 đồng và ngay lập tức lấy được bản mã trước khi An gửi tới ngân hàng. Giả sử bản mã là

```
10111100 01100001
```

Bình nên sửa bản mã như thế nào để sau khi giải mã nhận được đúng 32 đồng?

10. lý do mà hệ mã đối xứng với CTR-mode bị tấn công như trong Bài tập 9 là kẻ tấn công có thể tạo ra bản mã hợp lệ mà không cần dùng khoá k. Bạn hãy mô tả một sơ đồ mã hoá kết hợp với MAC (S, V) để kẻ tấn công không thể tạo ra bản mã c hợp lệ, tức là $\mathsf{V}(k, c) = 1$, khi không biết khoá bí mật k; và do đó có thể chống lại kiểu tấn công này.