NGÂN HÀNG CÂU HỎI THI TỰ LUẬN

Tên học phần: Mật mã học **Mã học phần: ELE 1406**

Ngành đào tạo: Điện – Điện tử **Trình độ đào tạo: Đại học**

1. Ngân hàng câu hỏi thi

CÂU HỎI LOẠI 1 ĐIỂM

Câu 1.1. Nêu ưu nhược điểm của các hệ mật khoá bí mật.

Câu 1.2. Nêu ưu nhược điểm của các hệ mật khoá công khai

Câu 1.3. Mô tả sơ đồ chức năng của hệ thống truyền tin sử dụng mật mã khoá bí mật.

Câu 1.4. Mô tả sơ đồ chức năng của hệ thống truyền tin sử dụng mật mã khoá công khai.

Câu 1.5. Mô tả hệ mật mã dịch vòng.

Câu 1.6. Mô tả hệ mật Affine.

Câu 1.7. Mô tả hệ mật mã dòng

Câu 1.8. Định nghĩa đa thức nguyên thủy và giải thích phương trình đồng dư tạo m-dãy theo đa thức nguyên thủy.

Câu 1.9. Các ứng dụng của chữ ký số.

Câu 1.10. Khái niệm và các tính chất của hàm băm.

Câu 1.11. Phân loại và ứng dụng của hàm băm.

CÂU HỎI LOẠI 2 ĐIỂM

Câu 2.1. Tính khoá chung trong thủ tục thoả thuận khoá Diffie – Hellman với $p=11,\alpha=7$, giả sử A chọn $x=4$, B chọn $y=7$.

Câu 2.2. Tính khoá chung trong thủ tục thoả thuận khoá Diffie – Hellman với $p=13,\alpha=11$, giả sử A chọn $x=7$, B chọn $y=5$.

Câu 2.3. Tính khoá chung trong thủ tục thoả thuận khoá Diffie – Hellman với $p=17,\alpha=10$, giả sử A chọn $x=3$, B chọn $y=5$.

Câu 2.4. Tính khoá chung trong thủ tục thoả thuận khoá Diffie – Hellman với $p=19,\alpha=3$, giả sử A chọn $x=13$, B chọn $y=11$.

Câu 2.5. Thực hiện truyền khóa bảo mật k từ A đến B bằng hệ mật Omura – Massey, với:

$p = 17$, khóa k = 7, giả sử cặp số bí mật của A là: (3,11) và của B là (5,13).

Câu 2.6. Thực hiện truyền tin bảo mật từ A đến B bằng hệ mật Omura – Massey, với:

$p = 19$ khóa k = 6, giả sử cặp số bí mật của A là: (5,11) và của B là (7,13).

Câu 2.7. Thực hiện truyền tin bảo mật từ A đến B bằng hệ mật Omura – Massey, với:

$p = 23$ khóa k = 6, giả sử cặp số bí mật của A là: (7,19) và của B là (5,9).

Câu 2.8. Thực hiện truyền tin bảo mật từ A đến B bằng hệ mật Omura – Massey, với:

$p = 23$ khóa k = 5, giả sử cặp số bí mật của A là: (13,17) và của B là (3,15).

Câu 2.9. Mô tả tóm tắt sơ đồ băm Matyas – Oseas và sơ đồ Davies – Mayer, điểm khác biệt cơ bản giữa hai sơ đồ này.

Câu 2.10. Các phương pháp đảm bảo tính toán vẹn của dữ liệu.

Câu 2.11. Mô tả sơ đồ chữ ký số sử dụng hàm băm không khoá. Xây dựng sơ đồ chữ ký số không bảo mật dùng RSA.

Câu 2.12. Mô tả sơ đồ chữ ký số có bảo mật dùng RSA.

Câu 2.13. Mô tả sơ đồ xây dựng chữ ký kép. Ý nghĩa của chữ ký kép trong giao dịch điện tử an toàn.

Câu 2.14. Trình bày các chế độ hoạt động của DES.

Câu 2.15. Mô tả mô hình truyền tin bảo mật theo kiến trúc PGP.

CÂU HỎI LOẠI 3 ĐIỂM

Câu 3.1. Thám mã thu được bản mã sau của một hệ mật mã dịch vòng với khoá k chưa biết:

PSZI_QIERW_RIZIV_LEZMRK_XS_WEC_CSY_EVI_WSVVC

Với ký hiệu (_) là khoảng trắng (dấu space).

Hãy thực hiện thám mã bản mã trên bằng các phương pháp đã biết (tìm khoá vét cạn, thống kê và dựa trên các hiểu biết về ngôn ngữ). Giả sử bản rõ là một văn bản tiếng Anh.

Câu 3.2. Thám mã thu được bản mã sau của một hệ mật mã dịch vòng với khoá k chưa biết:

TPIEWI_WSQI_GVC_SJ_QC_LIEVX_AMPP_FVIEO

Với ký hiệu (_) là khoảng trống (dấu space).

Hãy thực hiện thám mã bản mã trên bằng các phương pháp đã biết (tìm khoá vét cạn, thống kê và dựa trên các hiểu biết về ngôn ngữ). Giả sử bản rõ là một văn bản tiếng Anh.

Câu 3.3. Hãy thực hiện thám mã bản mã dưới bằng các phương pháp đã biết (tìm khoá vét cạn, thống kê và dựa trên các hiểu biết về ngôn ngữ). Giả sử bản mã là hệ mật mã dịch vòng và bản rõ là một văn bản tiếng Anh, ký hiệu (_) là khoảng trắng (dấu space).

RFS_NX_YMJ_RTXY_NSYJQQNLJSY_TK_YMJ_FSNRFQX_FSI_YMJ_RTXY_XNQQD

Câu 3.4. Hãy thực hiện thám mã bản mã dưới bằng các phương pháp đã biết (tìm khoá vét cạn, thống kê và dựa trên các hiểu biết về ngôn ngữ). Giả sử bản mã là hệ mật mã dịch vòng và bản rõ là một văn bản tiếng Anh, ký hiệu (_) là khoảng trắng (dấu space).

YMJ_KTTQNXM_RFS_XJJPX_MFUUNSJXX_NS_YMJ_INXYFSHJ_YMJ_BNXJ_ LWTBX_NY_ZSIJW_MNX_KJJY

Câu 3.5. Hãy thực hiện thám mã bản mã dưới bằng các phương pháp đã biết (tìm khoá vét cạn, thống kê và dựa trên các hiểu biết về ngôn ngữ). Giả sử bản mã là hệ mật mã dịch vòng và bản rõ là một văn bản tiếng Anh, ký hiệu (_) là khoảng trắng (dấu space).

APTL_PZ_TVYL_CHSBHISL_AOHU_TVULF_FVB_JHU_NLA_TVYL_TVULF_IBA_ FVB_JHUUVA_NLA_TVYL_APTL

Câu 3.6. Thám mã thu được bản mã sau của một hệ mật mã dịch vòng với khoá K chưa biết:

PACGHJUHHCRICGRFWRUCRICPHGLFLQH

Hãy thực hiện thám mã bản mã trên bằng các phương pháp

- Tìm khoá vét cạn.

- Thống kê (biết rằng các ký tự có xác suất xuất hiện lớn trong tiếng Anh được sắp xếp theo thứ tự sau: **_ , E, T, A, H, O, N ,** với giả sử ‘‘dấu cách’’ (_) được xem là 1 ký tự.

Câu 3.7. Thám mã thu được bản mã sau của một hệ mật mã dịch vòng với khoá k chưa biết:

RCEIJLWJJETKEITHYTWETKERJINHNSJ

Hãy thực hiện thám mã bản mã trên bằng các phương pháp

- Tìm khoá vét cạn

- Thống kê (biết rằng các ký tự có xác suất xuất hiện lớn trong tiếng Anh được sắp xếp theo thứ tự sau:

_ , E, T, A, H, O, N

Với giả sử ‘‘khoảng trống’’ (_) được xem là 1 ký tự

Câu 3.8. Thám mã thu được bản mã sau của một hệ mật mã dịch vòng với khoá k chưa biết:

LID_LSDMWDRSXDIZIVBHEBDGSRUYIVMRKDWSQIDJIEVDLEWDRSXDP
IEVRIHDXLIDWIGVIXDSJDPMJI

Hãy thực hiện thám mã bản mã trên bằng các phương pháp:

- Tìm khoá vét cạn

- Thống kê (biết rằng các ký tự có xác suất xuất hiện lớn trong tiếng Anh được sắp xếp theo thứ tự sau:

_ , E, T, A, H, O, N

Với giả sử ‘‘khoảng trống’’ (_) được xem là 1 ký tự.

Câu 3.9. Thực hiện thám mã bản mã sau của một hệ mật mã dịch vòng với khoá k chưa biết, bằng các phương pháp tìm khóa vét cạn và thống kê, biết rằng các ký tự có xác suất xuất hiện lớn trong tiếng Anh được sắp xếp theo thứ tự sau:

_,E,T,A,H,O,N

Với giả sử ‘‘khoảng trống’’ (**_**) được xem là 1 ký tự

XMQIDMWDQSVIDZEPYEFPIDXLERDQSRIBDBSYDGERDKIXDQSVIDQSRIBDFYX
DBSYDGERRSXDKIXDQSVIDXMQI

Câu 3.10. Thực hiện thám mã bản mã sau của một hệ mật mã dịch vòng với khoá k chưa biết, bằng các phương pháp tìm khóa vét cạn và thống kê, biết rằng các ký tự có xác suất xuất hiện lớn trong tiếng Anh được sắp xếp theo thứ tự sau:

_,E,T,A,H,O,N

Với giả sử ‘‘khoảng trống’’ (**_**) được xem là 1 ký tự

YMJEKTTQNXMERFSEXJJPXEMFUUNSJXXENSEYMJEINXYFSHJEYMJ
EANXJELWTAXENYEZSIJWEMNXEKJJY

Câu 3.11. Thực hiện thám mã bản mã sau của một hệ mật mã dịch vòng với khoá k chưa biết, bằng các phương pháp tìm khóa vét cạn và thống kê, biết rằng các ký tự có xác suất xuất hiện lớn trong tiếng Anh được sắp xếp theo thứ tự sau:

_,E,T,A,H,O,N

Với giả sử ‘‘khoảng trống’’ (**_**) được xem là 1 ký tự

ZNKFZX_KFYOMTFULFOTZKRROMKTIKFOYFTUZFQTUBRKJMKFH_ZFOSGMOTGZOUT

Câu 3.12. Thực hiện thám mã bản mã sau của một hệ mật mã dịch vòng với khoá k chưa biết, bằng các phương pháp tìm khóa vét cạn và thống kê, biết rằng các ký tự có xác suất xuất hiện lớn trong tiếng Anh được sắp xếp theo thứ tự sau:

_,E,T,A,H,O,N

Với giả sử ‘‘khoảng trống’’ (**_**) được xem là 1 ký tự

_IDRIZIVDORS_DXLIDPSZIDSJDSYVDTEVIRXWD
JSVDYWDXMPPD_IDLEZIDFIGSQIDTEVIRXW

Câu 3.13. Thám mã thu được bản mã sau:

-EHOHWSI-ON-E-TREVADYC-YQNOREUGNIOS--

EMAEFH-R-SATONEL-NRA-DEEHTES-ERCO-TL-FEFI

Hãy chỉ ra rằng đây là một hệ mật hoán vị và thực hiện thám mã bằng phương pháp tìm khoá vét cạn (Ký hiệu (**-**) là dấu trắng).

Câu 3.14. Thám mã thu được bản mã sau

-AMNTSI-MEH--SOTENITGLLI-NETTFO-AEH-AINMASL-TDN-MEH--
SOTLISL--Y-

Hãy chỉ ra rằng đây là một hệ mật hoán vị và thực hiện thám mã bằng phương pháp tìm khoá vét cạn (Ký hiệu (**-**) là dấu trắng).

Câu 3.15. Hãy xây dựng M dãy với đa thức nguyên thuỷ $g(x)=1+x+x^4$ và đa thức mầm $b(x)=1+x$. Biết rằng phương trình tạo M dãy có dạng $a(x)\equiv b(x).x^i \bmod g(x)$; $i=0,1,2...$

Câu 3.16. Hãy xây dựng M dãy với đa thức nguyên thuỷ $g(x)=1+x^3+x^4$ và đa thức mầm $b(x)=1+x$. Biết rằng phương trình tạo M dãy có dạng $a(x)\equiv b(x).x^i \bmod g(x)$; $i=0,1,2...$

Câu 3.17.

a) Hãy tạo M dãy theo phương trình đồng dư sau:

$$a(x)\equiv b(x).c^i(x) \bmod (1+x+x^2+x^3+x^4);\ i=1,2,....$$

với đa thức mầm $b(x)=1$ và $c(x)=1+x^2+x^4 \leftrightarrow (024)$

b) Tìm tất cả các đa thức nguyên thuỷ có $ord\big(c(x)\big)=15$ trong dãy này.

Câu 3.18.

a) Hãy tạo M dãy theo phương trình đồng dư sau:

$$a(x)\equiv b(x).c^i(x) \bmod (1+x+x^2+x^3+x^4);\ i=1,2,....$$

với đa thức mầm $b(x)=1+x$ và $c(x)=1+x+x^2 \leftrightarrow (012)$

b) Tìm tất cả các đa thức nguyên thuỷ có $ord\big(c(x)\big)=15$ trong dãy này.

Câu 3.19. Cho hệ mật RSA với $p=13, q=17$

a) Tính n, $\varphi(n)$?

b) Tính d biết $e=19$.

c) Mã hoá cho bản tin $M=7$ bằng thuật toán nhân và bình phương.

Câu 3.20. Cho hệ mật RSA với $p=19, q=17$

a) Tính n, $\varphi(n)$?

b) Tính d biết $e=91$.

c) Mã hoá cho bản tin $M=6$ bằng thuật toán nhân và bình phương.

Câu 3.21. Cho hệ mật RSA với $p=19, q=23$

a) Tính n, $\varphi(n)$?

b) Tính d biết $e=41$.

c) Mã hoá cho bản tin $M=9$ bằng thuật toán nhân và bình phương.

Câu 3.22. Cho hệ mật RSA với $p=23, q=29$

a) Tính n, $\varphi(n)$?

b) Tính d biết $e=29$.

c) Mã hoá cho bản tin $M=8$ bằng thuật toán nhân và bình phương.

Câu 3.23. Xây dựng hệ mật ElGamal truyền tin bảo mật từ B đến A.

a) Hãy xây dựng khóa công khai cho A, với $p=17$ và $\alpha=3$ là phần tử nguyên thủy của $\mathbb{Z}_{17}^*$, giả sử khóa bí mật của A là $a=6$.

b) Giả sử B chọn số ngẫu nhiên $k=4$, hãy mã hoá bản tin $M=7$ gửi từ B đến A bằng khóa công khai tại phần a).

c) Hãy thực hiện giải mã tại bên A để tìm lại bản rõ M ở phần b).

Câu 3.24. Xây dựng hệ mật ElGamal truyền tin bảo mật từ B đến A.

a) Hãy xây dựng khóa công khai cho A, với $p=17$ và $\alpha=11$ là phần tử nguyên thủy của $\mathbb{Z}_{17}^*$, giả sử khóa bí mật của A là $a=5$.

b) Giả sử B chọn số ngẫu nhiên $k=7$, hãy mã hoá bản tin $M=8$ gửi từ B đến A bằng khóa công khai tại phần a).

c) Hãy thực hiện giải mã tại bên A để tìm lại bản rõ M ở phần b).

Câu 3.25. Xây dựng hệ mật ElGamal truyền tin bảo mật từ B đến A.

a) Hãy xây dựng khóa công khai cho A, với $p = 19$ và $\alpha = 13$ là phần tử nguyên thủy của $\mathbb{Z}_{19}^*$, giả sử khóa bí mật của A là $a = 4$.

b) Giả sử B chọn số ngẫu nhiên $k = 5$, hãy mã hoá bản tin $M = 7$ gửi từ B đến A bằng khóa công khai tại phần a).

c) Hãy thực hiện giải mã tại bên A để tìm lại bản rõ M ở phần b).

Câu 3.26. Xây dựng hệ mật ElGamal truyền tin bảo mật từ B đến A.

a) Hãy xây dựng khóa công khai cho A, với $p = 19$ và $\alpha = 14$ là phần tử nguyên thủy của $\mathbb{Z}_{19}^*$, giả sử khóa bí mật của A là $a = 6$.

b) Giả sử B chọn số ngẫu nhiên $k = 5$, hãy mã hoá bản tin $M = 4$ gửi từ B đến A bằng khóa công khai tại phần a).

c) Hãy thực hiện giải mã tại bên A để tìm lại bản rõ M ở phần b).

Câu 3.27. Cho $\mathbb{Z}_{13}$, biết $\alpha = 2$ là phần tử nguyên thuỷ của $\mathbb{Z}_{13}^*$. Hãy:

a) Tìm tất cả các phần tử nguyên thuỷ của $\mathbb{Z}_{13}^*$

b) Giải bài toán logarit rời rạc: Tìm $\log_\alpha y$ với α là phần tử nguyên thuỷ và $y \in \mathbb{Z}_{13}^*$

c) Tìm các thặng dư bậc 2 của $\mathbb{Z}_{13}^*$

Câu 3.28. Cho $\mathbb{Z}_{17}$, biết $\alpha = 3$ là phần tử nguyên thuỷ của $\mathbb{Z}_{17}^*$. Hãy:

a) Tìm tất cả các phần tử nguyên thuỷ của $\mathbb{Z}_{17}^*$

b) Giải bài toán logarit rời rạc: Tìm $\log_\alpha y$ với α là phần tử nguyên thuỷ và $y \in \mathbb{Z}_{17}^*$

c) Tìm các thặng dư bậc 2 của $\mathbb{Z}_{17}^*$

Câu 3.29. Cho $\mathbb{Z}_{11}$, biết $\alpha = 2$ là phần tử nguyên thuỷ của $\mathbb{Z}_{11}^*$. Hãy

a) Tìm tất cả các phần tử nguyên thuỷ của $\mathbb{Z}_{11}^*$

b) Giải bài toán logarit rời rạc: Tìm $\log_\alpha y$ với α là phần tử nguyên thuỷ và $y \in \mathbb{Z}_{11}^*$

c) Tìm các thặng dư bậc 2 của $\mathbb{Z}_{11}^*$

Câu 3.30. Cho $\mathbb{Z}_{19}$, biết $\alpha = 2$ là phần tử nguyên thuỷ của $\mathbb{Z}_{19}^*$. Hãy

a) Tìm tất cả các phần tử nguyên thuỷ của $\mathbb{Z}_{19}^*$

b) Giải bài toán logarit rời rạc: Tìm $\log_\alpha y$ với α là phần tử nguyên thuỷ và $y \in \mathbb{Z}_{19}^*$

c) Tìm các thặng dư bậc 2 của $\mathbb{Z}_{19}^*$

CÂU HỎI LOẠI 4 ĐIỂM

Câu 4.1. Cho đường cong Elliptic $y^2 = x^3 + x + 1 \bmod 13$

Hãy xây dựng nhóm E_{13} với $P = (1,4)$ là phần tử nguyên thuỷ (tìm các điểm của E_{13}). Tìm tất cả các phần tử nguyên thuỷ.

Câu 4.2. Cho đường cong Elliptic $y^2 = x^3 + x + 1 \bmod 13$

Hãy xây dựng nhóm E_{13} với $P = (5,1)$ là phần tử nguyên thuỷ (tìm các điểm của E_{13}). Tìm tất cả các phần tử nguyên thuỷ.

Câu 4.3. Cho đường cong Elliptic $y^2 = x^3 + x + 6 \bmod 17$

Hãy xây dựng nhóm E_{17} với $P = (2,4)$ là phần tử nguyên thuỷ (tìm các điểm của E_{17}). Tìm tất cả các phần tử nguyên thuỷ.

Câu 4.4. Cho đường cong Elliptic $y^2 = x^3 + x + 1 \bmod 17$

Hãy xây dựng nhóm E_{17} với $P = (0,1)$ là phần tử nguyên thuỷ (tìm các điểm của E_{17}). Tìm tất cả các phần tử nguyên thuỷ.

Câu 4.5. Cho đường cong Elliptic $y^2 = x^3 + x + 1 \bmod 11$

Hãy xây dựng nhóm E_{11} với $P = (1,5)$ là phần tử nguyên thuỷ (tìm các điểm của E_{11}). Tìm tất cả các phần tử nguyên thuỷ.

Câu 4.6. Cho đường cong Elliptic $y^2 = x^3 + x + 3 \bmod 11$

Hãy xây dựng nhóm E_{11} với $P = (5,1)$ là phần tử nguyên thuỷ (tìm các điểm của E_{11}). Tìm tất cả các phần tử nguyên thuỷ.

Câu 4.7. Cho đường cong Elliptic $y^2 = x^3 + x + 1 \bmod 11$

Hãy xây dựng nhóm E_{11} với $P = (4,6)$ là phần tử nguyên thuỷ (tìm các điểm của E_{11}). Tìm tất cả các phần tử nguyên thuỷ.

Câu 4.8. Cho đường cong Elliptic $y^2 = x^3 + x + 3 \bmod 11$

Hãy xây dựng nhóm E_{11} với $P = (9,2)$ là phần tử nguyên thuỷ (tìm các điểm của E_{11}). Tìm tất cả các phần tử nguyên thuỷ.

2. Đề xuất các phương án tổ hợp câu hỏi thi thành các đề thi

Phương án 1:

- 1 câu 1 điểm.
- 1 câu 2 điểm.
- 1 câu 3 điểm.
- 1 câu 4 điểm.

Phương án 2:

- 2 câu 1 điểm.
- 1 câu 2 điểm.
- 2 câu 3 điểm **(*1 câu nằm trong các câu từ 3.1 đến 3.14; và 1 câu nằm trong các câu từ 3.15 đến 3.30*)**

Phương án 2:

- 2 câu 2 điểm.
- 2 câu 3 điểm **(*1 câu nằm trong các câu từ 3.1 đến 3.14; và 1 câu nằm trong các câu từ 3.15 đến 3.30*).**

3. Hướng dẫn cần thiết khác:

Ngân hàng câu hỏi thi này đã được thông qua bộ môn và nhóm cán bộ giảng dạy học phần.

Hà Nội, ngày . . . tháng 11 năm 2013

Trưởng khoa	**Trưởng bộ môn**	**Giảng viên chủ trì biên soạn**
TS. Đặng Hoài Bắc		**GS.TS Nguyễn Bình**