ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

ĐỀ THI CUỐI KỲ NM AN TOÀN THÔNG TIN
HỌC KỲ II NĂM HỌC 2019-2020

ĐỀ SỐ 1
THỜI GIAN: 90'

Câu 1. a)Cho hệ mật có ba khóa $\{k_1, k_2, k_3\}$, ba bản rõ $\{m_1, m_2, m_3\}$ và bốn bản mã $\{c_1, c_2, c_3, c_4\}$, với sơ đồ mã hóa như sau:

	m_1	m_2	m_3
k_1	c_2	c_4	c_1
k_2	c_1	c_3	c_2
k_3	c_3	c_1	c_2

Giả sử rằng phân phối xác xuất của không gian các bản rõ và khóa như sau: $P(m_1) = P(m_2) = 0.4$; $P(m_3) = 0.2$. $P(k_1) = P(k_2) = P(k_3) = 1/3$.

Hệ mật này có phải hệ mật hoàn thiện (hệ mật bí mật hoàn toàn) hay không?

b) Hãy giải mã bản mã sau QZNHOBXZD, biết rằng nó được mã bởi hệ mật Affine với a=5 và b=7. Số khóa có thể của hệ mật Affine bằng bao nhiêu?

Câu 2. Cho hệ mật RSA với p = 61, q=79, n=p*q và số e=2501. Hãy:

a) Tính $d = e^{-1} \bmod \Phi(n)$, (trình bày đầy đủ các bước tính toán).

b) Mã hóa bản tin x=BC sau đó giải mã bản mã nhận được. Phép mã hóa và giải mã trình bày đầy đủ các bước.

c) Hãy trình bày ba các cách tấn công hệ mật RSA mà anh/chị biết.

Câu 3. Cho đường cong $E_{29}(-1,16): y^2 \equiv x^3 - x + 16 \pmod{29}$, có danh sách các điểm như sau và điểm vô cực O:

P	2P	3P	4P	5P	69	7P	8P	9P	10P
(5, 7)	(28, 4)	(18, 1)	(22, 12)	(6, 20)	(13, 5)	(2, 14)	(21, 11)	(23, 3)	(10, 7)
11P	12P	13P	14P	15P	169	17P	18P	19P	20P
(14, 22)	(16, 23)	(7, 27)	(1, 4)	(0, 4)	(0, 25)	(1, 25)	(7, 2)	(16, 6)	(14, 7)
21P	22P	23P	24P	25P	269	27P	28P	29P	30P
(10, 22)	(23, 26)	(21, 18)	(2, 15)	(13, 24)	(6, 9)	(22, 17)	(18, 28)	(28, 25)	(5, 22)

a) Hãy trình bày sơ đồ chữ ký trên đường cong Elliptic (ECDSA).

b) Cho hệ mật ECC được xây dựng trên đường cong elliptic $E_{29}(-1,16)$ cho ở trên với điểm cơ sở A= 5P và khóa bí mật d=12. Sử dụng hệ mật này và áp dụng phần a) để ký trên văn bản x có giá trị băm h(x)=21 và khóa đệm k_E=25.

c) Kiểm thử chữ ký thu được ở phần b).

Chúc các anh/chị thi tốt!

$$P(x|y) = \frac{P(y|x)\,P(x)}{P(y)}$$

$$P(m|c) = \frac{P(c|m)\,P(m)}{}$$