T-79.5501 Cryptology
EXAM
Thursday, May 26, 2011

1. Let us suppose that $\mathbf{Pr}[y] > 0$, for all $y \in \mathcal{C}$.

   (a) (2 pts) Prove that the cryptosystem achieves perfect secrecy if and only if $\mathbf{P}$ and $\mathbf{C}$ are independent random variables.

   (b) (4 pts) Suppose that, for each pair (x, y), $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there is exactly one key $K \in \mathcal{K}$ such that $e_K(x) = y$, that is, $H(\mathbf{K}|\mathbf{PC}) = 0$. Prove that then the cryptosystem achieves perfect secrecy if and only if $H(\mathbf{K}) = H(\mathbf{C})$.

2. Let $\alpha = (010) \in GF(2^3)$ with polynomial $x^3 + x + 1$. Consider function $f : \mathbb{Z}_8 \to \{0,1\}$ defined as

$$f(u) = \begin{cases} \text{msb}(\alpha^u), \text{ for } u \neq 7 \\ 0, \text{ for } u = 7 \end{cases}$$

   where msb denotes the most significant bit. By identifying $u = u_3 2^2 + u_2 2 + u_1 \in \mathbb{Z}_8$ with $(u_3, u_2, u_1) \in \{0,1\}^3$, the function f is defined from $\{0,1\}^3$ to $\{0,1\}$.

   (a) (3 pts) Compute the truth table of f.

   (b) (3 pts) Compute the algebraic normal form ANF of f.

3. (6 pts) Bob and Bart are using the *Rabin Cryptosystem*. Bob's modulus is 2183 and Bart's modulus is 2279. Alice wants to send an integer x, $0 < x < 2183$, encrypted to both of them. She sends ciphertext 1479 to Bob and the ciphertext 418 to Bart. Carol sees the ciphertexts and she knows Bob's and Bart's moduli. Show how Carol can compute x without factoring of moduli.

4. (a) (2 pts) Numbers $p = 2011$ and $q = 67$ are prime. Show that $\alpha = 3^{30} \bmod 2011 = 1116$ has multiplicative order 67 in $\mathbb{F}_{2011}$.

   (b) (4 pts) Find $x \in \mathbb{Z}_{67}$ such that

$$1116 \cdot (1116^x)^x \equiv 462 \pmod{2011}.$$

   Hint: $1116^{-1} \bmod 2011 = 182$, $1116^9 \bmod 2011 = 754$.

5. Let us consider the elliptic curve $E = E(\mathbb{F}_{23}) : y^2 = x^3 + 2x + 19$. Its points are given in the table below generated by the point $P = (10, 2)$.

i	iP	i	iP	i	iP	i	iP
1	(10,2)	7	(22,19)	13	(19,19)	19	(3,12)
2	(5,19)	8	(20,3)	14	(20,20)	20	(5,4)
3	(3,11)	9	(19,4)	15	(22,4)	21	(10,21)
4	(14,13)	10	(2,10)	16	(7,10)	22	$\mathcal{O}$
5	(8,15)	11	(12,0)	17	(8,8)		
6	(7,13)	12	(2,13)	18	(14,10)		

   (a) (2 pts) E has a cyclic subgroup G of order 11. Which points generate this subgroup?

   (b) (2 pts) Let $a = 3$ be a private key in ElGamal cryptosystem in G with generator $Q = (20, 20)$. Compute the public key.

   (c) (2 pts) Using $k = 4$ as the secret nonce and the public key computed above, compute the ElGamal encryption of the point $(2, 10)$.

Exam Calculator Policy. It is allowed to use a function calculator, however no programmable calculator.
Course Feedback. Please give your feedback at:
http://www.cs.hut.fi/cgi-bin/teekysely.pl?action=showform&id=T795501-T795501-k2011palaute&lang=ENG