T-79.4502 Cryptography and Data Security (5 cr)

EXAM
Thursday, February 18, 2016
Five problems, two pages!

1. The *Autokey cipher* over the alphabet $\mathbb{Z}_{26}$ is defined as follows. Given a key $\kappa \in \mathbb{Z}_{26}$, the plaintext $x = (x_1, \ldots, x_n) \in \mathbb{Z}_{26}^n$, $n \geq 1$ is encrypted to ciphertext $y = (y_1, \ldots, y_n)$ as follows

$$\begin{aligned} y_1 &= x_1 + \kappa \bmod 26, \text{ and} \\ y_i &= x_i + x_{i-1} \bmod 26, \text{ for } i = 2, 3, \ldots, n. \end{aligned}$$

   (a) (3 pts) The attacker sees the ciphertext, and transforms it to sequence $z = (z_1, \ldots, z_n)$ as follows:

$$\begin{aligned} z_1 &= y_1, \text{ and} \\ z_i &= y_i - z_{i-1} \bmod 26, \text{ for } i = 2, 3, \ldots, n. \end{aligned}$$

   Show that then z is equal to the ciphertext obtained by encrypting x using the 2-periodic Vigenère cipher with keyword $\kappa, -\kappa$, which means that

$$\begin{aligned} z_i &= x_1 + \kappa \bmod 26, \text{ for } i \text{ odd}, \\ z_i &= x_i - \kappa \bmod 26, \text{ for } i \text{ even}. \end{aligned}$$

   (b) (3 pts) The following ciphertext is obtained from an English text by using the *Autokey cipher*

```
G A L E R I Z D V L Z T Y A L G Q Z O G D R B D F B K

U U E V G X V E R S W F 1 H F Q E N Y T N J W L H D H
```

   It is given that $\kappa =$ E or N or T. Find κ.
   Here is the conversion from letters to numbers:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. (6 pts) Let us consider a 4-bit S-box S defined as follows:

x	$S(x)$
$0 = 0000_2$	a $= 1010_2$
$1 = 0001_2$	$6 = 0110_2$
$2 = 0010_2$	$9 = 1001_2$
$3 = 0011_2$	$0 = 0000_2$
$4 = 0100_2$	c $= 1100_2$
$5 = 0101_2$	b $= 1011_2$
$6 = 0110_2$	$7 = 0111_2$
$7 = 0111_2$	d $= 1101_2$
$8 = 1000_2$	f $= 1111_2$
$9 = 1001_2$	$1 = 0001_2$
a $= 1010_2$	$3 = 0011_2$
b $= 1011_2$	e $= 1110_2$
c $= 1100_2$	$5 = 0101_2$
d $= 1101_2$	$2 = 0010_2$
e $= 1110_2$	$8 = 1000_2$
f $= 1111_2$	$4 = 0100_2$

Given two 4-bit keys K_1 and K_2 and a 4-bit plaintext x we define an encryption function e_{K_1,K_2} such that

$$e_{K_1,K_2}(x) = S(S(x \oplus K_1) \oplus K_2).$$

An adversary sees two plaintexts $x = \texttt{0}$ and $x = \texttt{1}$ and the corresponding ciphertexts

$$e_{K_1,K_2}(\texttt{0}) = \texttt{e} \text{ and } e_{K_1,K_2}(\texttt{1}) = \texttt{5}.$$

Find secret keys K_1 and K_2 using the Meet-in-the-Middle method and the look-up table of S. Is the solution K_1 and K_2 unique?

3. (6 pts) Consider polynomial arithmetic in the set of 3-bit integers using polynomial $x^3 + x + 1$.
   (a) (3 pts) Determine the discrete logarithm of $6 = \texttt{110}$ to the base $2 = \texttt{010}$.
   (b) (3 pts) Calculate the inverse of $6 = \texttt{110}$.

4. Consider the following Boolean function of three binary variables a, b, c

$$f(a, b, c) = ab + bc + ac,$$

where '+' is the addition modulo 2 and $ab = 1$ if and only if $a = b = 1$.
   (a) (2 pts) Show that the probability that $f(a, b, c) = 0$ is equal to $1/2$, that is, the function $f(a, b, c)$ take value 0 and 1 equally many times as the input (a, b, c) takes all possible values.
   (b) (2 pts) Show that the probability that $f(a, b, c) = a$ is equal to $3/4$.
   (c) (2 pts) Assume that such a function has been used in a stream cipher construction to combine three secret sequences and that the set of possible first input sequences is known to the attacker. The attacker observes the output sequence. Explain how the attacker can use the property (b) to find the correct first input sequence.

5. Alice and Bob are using the Diffie-Hellman key exchange method in the multiplicative group $\mathbb{F}_{19}$ with a generator element $g = 2$. Unfortunately their communication channel is not properly authenticated and Mallory interferes in their communication and performs a Man-in-the-Middle attack. In this session, Alice sends her public key $A = 14$ and Bob sends his public key $B = 3$. Mallory uses $x = 3$ as his private exponent to compute his public key he sends to Alice and Bob.
   (a) (4 pts) What are the session keys that Alice and Bob then compute?
   (b) (2 pts) Explain what happens when Alice sends messages to Bob encrypted using her session key?

Exam Calculator Policy. It is allowed to use a function calculator, however no programmable calculator.