T-79.503 Foundations of Cryptology
Exam
December 10, 2004

SOLUTIONS

1. (6 points) There are m possible blocks with exactly one non-zero bit. They are all equally likely. It follows that the entropy of one block is $H(P) = \log_2(m)$. Since the blocks are chosen independently the entropy of the language is equal to

$$H_L = \lim_{n\to\infty} \frac{H(P^n)}{n} = \lim_{n\to\infty} \frac{nH(P)}{n} = H(P) = \log_2(m),$$

and from there the redundancy of the language is equal to

$$R_L = 1 - \frac{H_L)}{\log_2 2^m} = 1 - \frac{\log_2(m)}{m} = \frac{m - \log_2(m)}{m}.$$

The estimate of the unicity distance is now

$$n_0 \approx \frac{m}{R_L \cdot m} = \frac{m}{m - \log_2(m)}.$$

It follows that $n_0 \leq 2$ if and only if $\log_2(m) \leq m/2$. This holds for all positive integers except for $m = 3$, since $\log_2(3) \approx 1,585$.

2. If we decrypt y_1 and y_2 with the correct partial key K_2, we get $d_{K_2}(y_1) = x_1 \oplus K_1$ and $d_{K_2}(y_2) = x_2 \oplus K_1$. Hence for the correct key K_2 we have

$$d_{K_2}(y_1) \oplus d_{K_2}(y_2) = x_1 \oplus x_2.$$

Based on this observation we can test for a 64-bit key candidate Z whether the equality

$$d_Z(y_1) \oplus d_Z(y_2) = x_1 \oplus x_2.$$

holds. The correct key $Z = K_2$ always passes the test. The solution is unique if none of the other candidates passes the test. When estimating the probability that the solution is unique, we may assume that for a wrong key Z the value $d_Z(y_1) \oplus d_Z(y_2)$ is a value that is selected uniformly at random. The probability that it equals $x_1 \oplus x_2$ can therefore be assumed to be 2^{-64}. Hence the probability that none of the $2^{64} - 1$ wrong keys hits $x_1 \oplus x_2$ is approximately equal to

$$(1 - \frac{1}{2^{64}})^{2^{64}-1} \approx e^{-1}.$$

After K_2 is found, then K_1 can be computed as $K_1 = d_{K_2}(y_1) \oplus x_1$.

3. (6 points) The 3rd term of the ciphertext sequence is $y_3 = \beta^3 + x_3 = 0111 = x^2 + x + 1$. Given the nature of the plaintext language, it follows that exactly one of the following holds:

$$\begin{aligned} \beta^3 &= 1111 \\ \beta^3 &= 0011 \\ \beta^3 &= 0101 \\ \beta^3 &= 0110 \end{aligned}$$

An equation may give solutions for β only if the order of the element on the right hand side divides $|\mathbb{F}^*|/3 = 5$, or, what is equivalent, the element is in the image of the mapping $z \to z^3$ in $\mathbb{F}$. Let us compute the image of $z \to z^3$. We know that it has five different non-zero elements:

0001	0001
0010	$x^3 = 1000$
0011	$(x+1)^3 = x^3 + x^2 + x + 1 = 1111$
0100	$x^6 = x^2(x+1) = x^3 + x^2 = 1100$
0101	$\ldots = 1010$
0110	$\ldots$ =0001
0111	$\ldots = 0001$
1000	$(x^3)^3 = x(x+1)^2 = 1010$
1001	$(x^3+1)^3 = \ldots = 1111$
1010	$\ldots = 1111$
1011	$\ldots = 1100$
1100	$\ldots = 1000$
1101	$\ldots = 1010$
1110	$x^3(x^2+x+1)^3 = x^3 = 1000$
1111	$\ldots = 1100$

It follows that $\beta^3 = 1111$ and the three possible values of β are 0011, 1001 and 1010.

4. By Fermat's theorem (Corollary 5.6)

$$4815^{25} = 12^{50100} = 1 \,(\mathrm{mod} 50101).$$

It follows that the order of 4815 in $\mathbb{Z}^*_{50101}$ divides 25, and therefore it is equal to 1, 5 or 25. It cannot be equal to 1, since $4815 \neq 1 \,(\mathrm{mod} 50101)$. We compute $4815^5 = 46880 \neq 1 \,(\mathrm{mod} 50101)$ to see that the order of 4815 cannot be 5. It follows that the order is 25.

5. We use Shanks' algorithm with $\alpha = 4815$, $G =< \alpha >$ in $\mathbb{Z}^*_{50101}$, $n = 25$, and $\beta = 48794$. Then $m = \lceil \sqrt{25} \rceil = 5$, and $\alpha^m = 4815^5 = 46880 \,(\mathrm{mod} 50101)$. The first list L_1 is then as follows:

j	46880^j mod 50101
0	1
1	46880
2	3934
3	4139
4	45248

To compute the second list we compute first 4815^{-1} mod 50101.

6. The Extended Euclidean algorithm gives:

i	r_i	q_i	t_i
0	50101	-	0
1	4815	10	1
2	1951	2	-10
3	913	2	21
4	125	7	-52
5	38	3	385
6	11	3	-1207
7	5	2	4006
8	1		-9219

It follows that $4815^{-1} \bmod 50101 = -9219 = 40882$. Then

i	$48794 \cdot 4815^{-i} \bmod 50101$
0	48794
1	$48794 \cdot 40882 = 24993$
2	$24993 \cdot 40882 = 4032$
3	$4032 \cdot 40882 = 3934$
$\vdots$	$\vdots$

from where we see that the solution is $i = 3$ and $j = 2$ from where $x = j \cdot m + i = 2 \cdot 5 + 3 = 13$.