T-79.503 Foundations of Cryptology
Homework 1
September 23, 2004

1. A false GSM base station is an entity which can impersonate a GSM base station (BTS) to a mobile station (MS), but does not have connection to the home network of the GSM subscriber. A false GSM base station can also listen and record all traffic between the MS and BTS. The GSM security protocol is shown in the picture. IMSI and TMSI are MS identities, the responses XRES (= SRES) and the secret ciphering key Kc are computed from Ki and RAND using a one-way function (difficult to invert). Consider what kind of security problems a false base station can cause in the system.

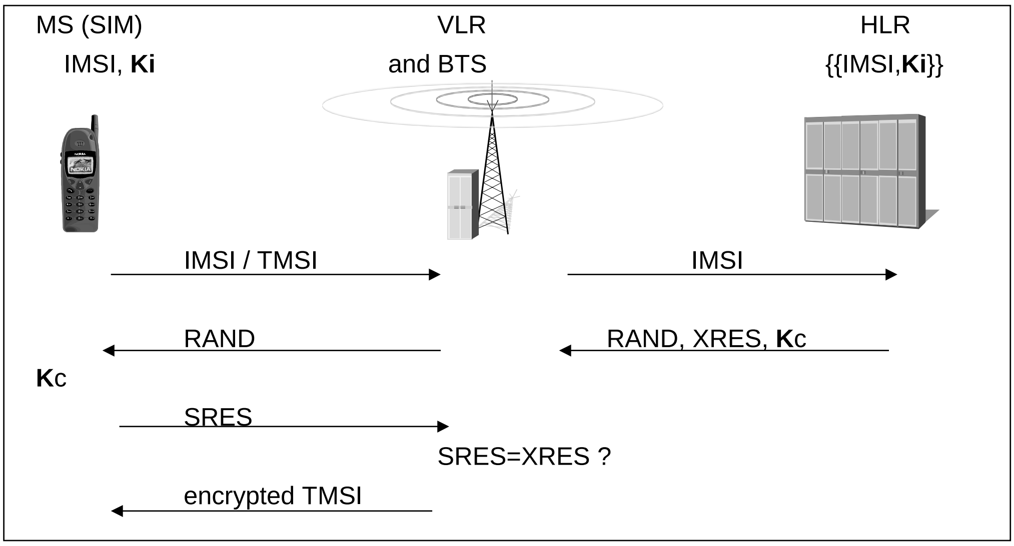

Figure 1: GSM Security Protocol

2. (Stinson 1.8) List all invertible elements in $\mathbb{Z}_m$, for m = 28, 33 and 35.

3. (Stinson 1.6 and 1.11 a)) If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an *involutory key*.

   a) Find all the involutory keys in the *Shift Cipher* over $\mathbb{Z}_{26}$.

   b) Suppose that $K = (a, b)$ is a key in an affine cipher over $\mathbb{Z}_n$. Prove that K is an involutory key if and only if $a^{-1} \bmod n = a$ and $b(a + 1) \equiv 0 (\bmod n)$.

4. This ciphertext is generated using a Vigenère cipher. Use Kasiski's method to find the period.

```
APWVC  DKPAK  BCECY  WXBBK  CYVSE  FVTLV  MXGRG
KKGFD  LRLZK  TFVKH  SAGUK  YEXSR  SIQTW  JXVFL
LALUI  KYABZ  XGRKL  BAFSG  CCMJT  ZDGST  AHBJM
MLGEZ  RPZIJ  XPVGU  OJXHL  PUMVM  CKYEX  SRSIQ
KCWMC  KFLQJ  FWJRH  SWLOX  YPVKM  HYCTA  WEJVQ
DPAVV  KFLKG  FDLRL  ZKIWT  IBXSG  RTPLL  AMHFR
OMEMV  ZQZGK  MSDFH  ATXSE  ELVWK  OCJFQ  FLHRJ
SMVMV  IMBOZ  HIKRO  MUNIE  RYG
```

5. (Stinson 1.15) Determine the inverses of the following matrices over $\mathbb{Z}_{26}$:

$$\text{a)} \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix} \quad \text{b)} \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$$

6. The plaintext and ciphertext alphabet consists of the 26 letters A-Z and the space between words. These 27 symbols are converted to integers modulo 27 as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	
0	1	2	3	4	5	6	7	8	9	10	11	12	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	"space"
13	14	15	16	17	18	19	20	21	22	23	24	25	26

Each plaintext character x is encrypted separately using a randomized substitution method. The key $K = (k_0, k_1, \ldots, k_9)$ is a permutation of the ten digits $\{0, 1, \ldots, 9\}$. The encryption process has the following steps.

(a) Pick a character y from the plaintext alphabet at random. Interpret the pair (y, x) as the representation of an integer I to the base 27, that is, $I = 27 \cdot y + x$. Let $a_2,\ a_1,\ a_0$ be the digits of I in the decimal system, where a_2 is the most significant digit.

(b) Use the key K to substitute a_i by k_{a_i}, $i = 0,\ 1,\ 2$.

(c) The ciphertext $(c_2,\ c_1,\ c_0)$ is obtained as the 27-base representation of the integer $100 \cdot k_{a_2} + 10 \cdot k_{a_1} + k_{a_0}$.

An attacker is observing plaintext-ciphertext pairs produced by this encryption method with the same fixed key. An encryption of the character 'space' is 'ABX' and an encryption for character 'B' is 'ACB'. Based on this information, derive a and b such that $k_a = 0$ and $k_b = 5$.