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

## SOLUTIONS

1. (a) IMSI-catching: A false base station can request for non-encryted IMSI, which is a unique identifier of the SIM.
   (b) RAND-replay: A false base station can record a used RAND, and at some later time resend it to the MS. In this manner it can force the MS to use the previously used encryption key.
   (c) Select a weak encryption algorithm: Base station selects the encryption algorithm in use.

   For example a recent attack by Barkan, Biham and Keller exploits (b) and (c). First they record a RAND and encrypted communication. At some later point they resend the RAND and tell to use a weak encryption algotithm. Then they derive the encryption key Kc, which is the same key, which was used in the first recorded ciphertext. Then they can decrypt the first ciphertext.

2.

$$\begin{aligned}
\mathbb{Z}_{28}^* &= \{1,3,5,9,11,13,15,17,19,23,25,27\} \\
\mathbb{Z}_{33}^* &= \{1,2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32\} \\
\mathbb{Z}_{35}^* &= \{1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34\}
\end{aligned}$$

3. (a) $K$ is an involutory key of the shift cipher over $\mathbb{Z}_{26}$ if and only is $e_K(e_K(x)) = x$, for all $x \in \mathbb{Z}_{26}$, that is, $(x+K)+K \equiv x \mod (26)$. This condition is satisfied if and only if $K = 0$ or $K = 13$.
   (b) $K = (a,b)$ is an involutory key in the affine cipher over $\mathbb{Z}_n$ if and only if $a(ax+b)+b \equiv x \pmod{n}$ for all $x \in \mathbb{Z}_n$. This condition is satisfied if and only if

$$\begin{aligned}
&a^2 \equiv 1 \pmod{n} \text{ and} \\
&ab + b \equiv 0 \pmod{n},
\end{aligned}$$

   from where the claim follows.

4. The most significant repetitions are `KGFDLRLZK` and `KYEXSRSIQ`. The distances are 147 and 77, respectively. Other shorter repetitions are, for example, `XGR`, `LLA` and `MVM`.

```
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
```

By Kasiski's method, the period is gcd(77,147) $= 7$.

5. a)

$$\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}^{-1} = (2 \cdot 5 - 9 \cdot 5)^{-1} \begin{pmatrix} 5 & 21 \\ 17 & 2 \end{pmatrix} = 23 \begin{pmatrix} 5 & 21 \\ 17 & 2 \end{pmatrix} = \begin{pmatrix} 11 & 15 \\ 1 & 20 \end{pmatrix}.$$

b)

$$\begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}^{-1} = \begin{pmatrix} 25 & 11 & 22 \\ 10 & 13 & 4 \\ 17 & 24 & 1 \end{pmatrix}$$

6. $\texttt{ABX} = 0 \cdot 27^2 + 1 \cdot 27 + 23 = 050$, and

$\texttt{ACB} = 0 \cdot 27^2 + 2 \cdot 27 + 1 = 055$.

From this we see that the "space" and B have been encrypted as follows:

$$\begin{aligned} \text{“space”} \mapsto 27y_1 + 26 &= 100a + 10b + a \mapsto k_a k_b k_a = 050 \\ \texttt{B} \mapsto 27y_2 + 1 &= 100a + 10b + b \mapsto k_a k_b k_b = 055. \end{aligned}$$

From the equations in the middle, we get the following system of congruences:

$$\begin{aligned} 101a + 10b &\equiv 26 (\mathrm{mod} 27) \\ 100a + 11b &\equiv 1 (\mathrm{mod} 27), \end{aligned}$$

which has the following unique solution $a = 2$ and $b = 4$.