~~Crey~~pt 1 Ü2 21. APR. 2011

5.) a.)

$A \in \mathbb{Z}_n^{m \times m}$ is invertible $\Leftrightarrow$ $\gcd(n, \det(A)) = 1$

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \in \mathbb{Z}_n^{m \times m}$$

It holds $A^{-1} = \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mm} \end{pmatrix} = \dfrac{adj(A)}{\det(A)}$

$$adj(A) = \begin{pmatrix} \tilde{a}_{11} & \cdots & \tilde{a}_{1m} \\ \vdots & \ddots & \vdots \\ \tilde{a}_{m1} & \cdots & \tilde{a}_{mm} \end{pmatrix}^T$$ with

$$\tilde{a}_{ij} = (-1)^{i+j} \left| \begin{array}{ccc|ccc} a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1m} \\ \vdots & \ddots & & & & \vdots \\ a_{i-1,1} & & & & & \\ \hline a_{i+1,1} & & & & & \\ \vdots & & & & \ddots & \vdots \\ a_{m1} & \cdots & & & \cdots & a_{mm} \end{array} \right|$$

i/j row/col skipped

$$\Rightarrow b_{ij} = \frac{1}{\det(A)} \tilde{a}_{ji} \pmod{n}$$

$\tilde{a}_{ji} \in \mathbb{Z}_n$ b_{ij} exists $\Leftrightarrow$ $\det(A)^{-1}$ exists

$\Leftrightarrow \gcd(n, \det(A)) = 1$

last equivalence: see next homework $\iff m=1$

b.)

$$M = \begin{pmatrix} 7 & 1 \\ 9 & 2 \end{pmatrix} \in \mathbb{Z}_{26}^{2\times 2}$$

$$\det(M) = 7\cdot 2 - 1\cdot 9 = 5 \Rightarrow \gcd(26,5)=1$$

with a.) M is revertible.

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \quad \text{if } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$k = \det(A)^{-1} (\bmod 26) \iff 5k = 26\cdot l + 1$$

$$26 \equiv 1 \bmod 5 \quad \Rightarrow 26\cdot 4 \equiv 4 \bmod 5$$
$$\Rightarrow 26\cdot 4 + 1 \equiv 0 \bmod 5$$

$$\Rightarrow k = \frac{26\cdot 4 + 1}{5} = \frac{25\cdot 4 + 5}{5} = 21$$

$$\Rightarrow M^{-1} = 21 \begin{pmatrix} 2 & -1 \\ -9 & 7 \end{pmatrix} = \underline{\underline{\begin{pmatrix} 16 & 5 \\ 19 & 17 \end{pmatrix}}} \quad (\bmod (26))$$

$$21\cdot 17 = 21\cdot 13 + 21\cdot 4 = \ldots$$

4.) a.) $\underline{c} = A\cdot \underline{m} \qquad \underline{m}(m_1, m_2, m_3) \qquad A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \in \mathbb{Z}_2^{3\times 3}$

$$\Rightarrow \underline{c} = (c_1, c_2, c_3) = (m_1 + m_2 + m_3,\ m_1 + m_2,\ m_1 + m_3)$$
$$= e(\underline{m})$$

4. b.)

E5.a.) $\Rightarrow$ $\gcd(m, \det(A)) \overset{!}{=} 1$

$$\det(A) = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} + 1 \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} + 1 \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}$$

$$= 1 + 1 + 1 = 1 \pmod 2$$

$\Rightarrow \gcd(2, 1) = 1 \overset{E5.a.)}{\Longrightarrow} A$ is invertible

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow[\substack{R_2+R_3 \\ R_1+R_2}]{R3} \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{R_1+R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right) \Rightarrow A^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$d(\underline{c}) = A^{-1} \cdot \underline{c}$$

E6.) a.) # of possible keys

substitution cipher. Keys are given as permutations over symbol alphabet Σ.

$|\Sigma| = n$

$\Rightarrow n!$ permutations, i.e., $n!$ keys

b.) affine ciphers with 26 symbols in alphabet $c_i = a \cdot m_i + b \pmod{26}$

$m_i = a^{-1}(c_i - b) \pmod{26}$

$\Rightarrow a^{-1}$ has to exist for decryption

lecture: a^{-1} exists, iff $\gcd(a, 26) = 1$

$26 = 2 \cdot 13 \Rightarrow S = \{a \mid \gcd(a,26)=1\}$
$= \{a \mid 2 \nmid a \wedge 13 \nmid a\} \subset \mathbb{Z}_{26}$

$\Rightarrow |S| = |\mathbb{Z}_{26}^*| = 26/2 - 1 = \underline{12}$

No restriction for b

$\Rightarrow 26 \cdot 12 = 312$ possible keys

c.) Permutation cipher with block length k
$\Rightarrow k!$ permutations. $\Rightarrow k!$ keys

E7.)

a.) $e_{k_2}(e_{k_1}(m)) = e_{k_3}(m)$

Subst. $\pi_3 = \pi_1 \circ \pi_2$, i.e., $x_i \to x_{\pi_2(\pi_1(i))} = x_{\pi_3(i)}$

Affine: $c_i' = a_1 \cdot m_i + b_1 \pmod n$
$c_i = a_2(a_1 \cdot m_i + b_1) + b_2 \pmod{(n)}$
$\Rightarrow c_i = a_1 \cdot a_2 \cdot m_i + a_2 b_1 + b_2 \pmod{26}$
$= a \cdot m_i + b$ with $a = a_1 \cdot a_2 \bmod 26$
$b = a_2 \cdot b_1 + b_2 \bmod (26)$

with $\gcd(a_1, n) = \gcd(a_2, n) = 1$

$\Rightarrow \gcd(a = a_1 \cdot a_2, n) = 1$

Perm. $\pi_3 = \pi_1 \circ \pi_2$, $m_i \to m_{\pi_2(\pi_1(i))} = m_{\pi_3(i)}$