Tutorial 13

Problem 1/

a) $n = 39$ letters

ℓ	A	B	E	F	G	H	L	N	P	R	S	U	V	Y	Z
N_ℓ	5	5	3	2	5	2	1	2	1	3	2	1	5	1	1

$$I_C = \frac{1}{n(n-1)} \sum_{\ell=0}^{25} N_\ell (N_\ell - 1) = \frac{1}{39 \cdot 38} \left(4 \cdot 5 \cdot 4 + 2 \cdot 3 \cdot 2 + 4 \cdot 2 \cdot 1 \right)$$

$$= \frac{100}{1482} = \frac{50}{741} \approx 0.06748$$

b) I_C is close to $\kappa_E = 0.0669$, so it is likely that it is a monoalphabetic cipher.

c) From the first four letters we see that the difference is ± 13, hence, we have a Caesar cipher with $k = 13$. Add or subtract $13 = k$ to the ciphertext values and substitute with corresponding letters, cf. help sheet.

d) Some types of attacks
- ciphertext-only attack
- Chosen-plaintext attack
- Chosen-ciphertext attack
- Brute-force attack
- Linear cryptanalysis

e) $P \in \{0,1\}^{k \times k}$. Each row (column) has sum 1.

f) c_0 initial vector, $n \in \mathbb{N}$

$c_n = e(m_n \oplus c_{n-1})$ is cipher-block chaining

Problem 2

$$H(X|Y) = -\sum_j P(Y=y_j) \sum_i P(X=x_i \mid Y=y_j) \log\left(P(X=x_i \mid Y=y_j)\right)$$

$$= \sum_j P(Y=y_j)\, H(X|Y=y_j)$$

a) $$H(\hat{C}|\hat{M}) = \sum_{M \in \mathcal{M}} P(\hat{M}=M)\, H(\hat{C} \mid \hat{M}=M)$$

$$H(\hat{C} \mid \hat{M}=M) = -\sum_{c \in \mathcal{C}} P(\hat{C}=c \mid \hat{M}=M) \cdot \log P(\hat{C}=c \mid \hat{M}=M)$$

$$= -\underbrace{(1-\varepsilon)\log(1-\varepsilon)}_{M=C} - 3 \cdot \underbrace{\frac{\varepsilon}{3}\log\left(\frac{\varepsilon}{3}\right)}_{M \neq C}$$

$$= -(1-\varepsilon)\log(1-\varepsilon) - \varepsilon \log(\varepsilon) + \varepsilon \log(3)$$

$$\Rightarrow H(\hat{C}|\hat{M}) = \underbrace{\sum_{M \in \mathcal{M}} P(\hat{M}=M)}_{=1} \cdot \underbrace{H(\hat{C}|\hat{M}=M)}_{\text{independant of } M}$$

$$= -(1-\varepsilon)\log(1-\varepsilon) - \varepsilon \log(\varepsilon) + \varepsilon \log(3) \qquad (1)$$

$$P(\hat{C}=C) = \sum_{M \in \mathcal{M}} P(\hat{M}=M) \cdot P(\hat{C}=c \mid \hat{M}=M)$$

$$= (1-\varepsilon) \cdot P(\hat{M}=c) + \frac{\varepsilon}{3} P(\hat{M} \neq c)$$

b) If $\hat{M}$ is uniformly distributed then

$P(\hat{C}=C) = (1-\varepsilon) \cdot \frac{1}{4} + \frac{\varepsilon}{3} \cdot \frac{3}{4} = \frac{1}{4}$, hence,

$\hat{C}$ is uniformly distributed. $\Rightarrow H(\hat{C}) = H(\hat{M}) = \log(4)$ (2)

$H(\hat{M} \mid \hat{C})$? It holds the chain rule :

$$H(\hat{M}) + H(\hat{C}|\hat{M}) = H(\hat{C}) + H(\hat{M} \mid \hat{C})$$

$$\Rightarrow \quad H(\hat{C}|\hat{M}) = H(\hat{M} \mid \hat{C}) = (1)$$

c) Calculate (2) - (1) ✓

d) $P(\hat{C}=C|\hat{M}=M)$ does not depend on $M \Rightarrow 1-\varepsilon = \frac{\varepsilon}{3} \Rightarrow \varepsilon = \frac{3}{4}$ ✓

Problem 3 / Prop 7.5:

a is PE modulo p $(\Leftrightarrow)$ $a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod p$ $\forall p_i$

where $p-1 = \prod_i p_i^{k_i}$ is the prime factorization of $p-1$

a) $p-1 = 179-1 = 178 = 2 \cdot 89$; $a = 2$

$a^2 \equiv 4 \pmod{179}$

$2^{89} \equiv \underbrace{((2^7)^2)^6}_{128} \cdot 2^5 \equiv ((95)^2)^3 \cdot 32 \equiv 75^2 \cdot 75 \cdot 32 \equiv 76 \cdot 73 \equiv -1 \pmod{179}$

$\Rightarrow$ 2a is PE modulo $p = 179$

b) First Alice calc. $u = a^{x_A} \bmod p$

$u \equiv 2^{23} \equiv 2^{14} \cdot \underbrace{2^9}_{512} \equiv 95 \cdot 154 \equiv 131 \pmod{179}$

$v \equiv 2^{31} \equiv 2^{23} \cdot 2^8 \equiv 131 \cdot 77 \equiv 63 \pmod{179}$

$31 \cdot 23 \bmod (p-1) = 1$

$v^{x_A} \equiv u^{x_B} \equiv (2^{31})^{23} \equiv 2^1 \equiv 2 \pmod{179}$

SQM 2^{23}

Bit	S	M
1	2	
0	4	–
1	16	32
1	129	79
1	155	131

2^{89} (from a)

Bit	S	M
1	2	
0	4	–
1	16	32
1	129	79
0	155	–
0	39	–
1	89	178

c) Oscar should use $z = 89$ and sends $u^z \bmod 179$ to Bob & $v^z \bmod 179$ to Alice.

$\Rightarrow$ The shared key is ± 1 as $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$

d) Exclude ± 1 as shared key.

Problem 4

a) $\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1) = 10 \cdot 12 = 120$

$d = e^{-1} \bmod \varphi(n) = e^{-1} \bmod 120 \quad e = 7$

Calculate $\gcd(7, 120) = 1 = x \cdot 120 - 17 \cdot 7$

$\Rightarrow d = 103 \quad \Rightarrow m = c^d \bmod n = 31^{103} \bmod 143$

Use square and multiply to calculate $m = 47$.

b) $e \in \mathbb{Z}^*_{\varphi(n)} = \{ k \in \mathbb{N} \mid k < \varphi(n) \wedge \gcd(k, \varphi(n)) = 1 \}$

$\Rightarrow |\mathbb{Z}^*_{\varphi(n)}| = \varphi(\varphi(n))$ [In general: $|\mathbb{Z}^*_m| = \varphi(m)$]

c) It is not possible that $p \cdot q \mid m$, as $m < p \cdot q = n$

Hence $\gcd(m, n) \in \{p, q\} \Rightarrow q = \frac{n}{p}$ or $p = \frac{n}{q}$ may be calculated and gcd by Euklid.

As in a) $d = e^{-1} \bmod \varphi(n)$ by EEA.

d) Eulers criterion: -1 is QR $\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1$

$\Leftrightarrow \frac{p-1}{2} = 2k$

$\Leftrightarrow p = 4k + 1$ ✓