Tel Aviv University 2/11/2016

# Introduction to Modern Cryptography (0368.3049) – Ex. 1

Benny Chor and Orit Moskovich

Submission in singles or pairs to Orr Fischer's Schreiber mailbox (289) until 16/11/2016, 23:59 (IST)

**- Appeals/missing grade issues: bdikacs AT gmail.com**
**- Issues regarding missing/unchecked assignments will be addressed only if a soft copy will be submitted on time to: crypto.f16 AT gmail.com.**
**Subject of the email: Ex.1, ID**

1. Below are two paragraphs taken from a famous speech, encrypted using a substitution encryption. Solve the substitution cipher. Explain the techniques you use, and describe all steps of your solution. The ciphertext is also available as a text file in the course's homepage. (The original message language is English.)

```
xmjsayl ogz yus dasovzmpg mn norkhl hkns uojs bsqmgzoal
snnsqyb qukhzasg pogzsa odmcy yus byassyb mn yus ympgbukxb
dsqocbs yusl uojs gm bqummhb ym em ym ma gm rmgsl ym
sgodhs yusr ym em ym bqummh ma gm xoasgyb oy umrs ym bss
yuoy yusl em ym bqummh dsqocbs dmyu xoasgyb kn yusas ds
ypm uojs ym pmav ym vssx yus norkhl ohkjs yukb hsozb ym
o dasovzmpg kg rmaoh byogzoazb ym og ohoarkge akbs kg
khhsekykroql ogz ym eampkge jkmhsgqs pukqu sacxyb gmy
mghl xmhkykqohhl dcy sjsalpusas hkns kg yus ympgbukxb
kb zogesamcb yusas kb gmy o zol yuoy emsb dl pkyumcy
bmrsdmzl dskge byoddsz ma obbochysz ogz jkmhsgqs kb
qoaaksz mcy mn yus ympgbukxb kgym yus pukys hkjkge oasob
xsmxhs oas onaokz ym pohv ohmgs kg yus byassyb onysa zoav
umcbsdasovkgeb ogz amddsaksb oas kgqasobkge zsbxkys yus
noqy yuoy yus zsoyu bsgysgqs qog gmp ds krxmbsz nma
bcqu mnnsgqsb zsoyu bsgysgqsb qoggmy qcas yus nsbysakge bmas

zcakge rl hknsykrs k uojs zszkqoysz rl hkns ym yukb byaceehs
mn yus onakqog xsmxhs k uojs nmceuy oeokgby pukys zmrkgoykmg
ogz k uojs nmceuy oeokgby dhoqv zmrkgoykmg k uojs qusakbusz yus
kzsoh mn o zsrmqaoykq ogz nass bmqksyl kg pukqu ohh xsabmgb pkhh
hkjs ymesyusa kg uoarmgl ogz pkyu sicoh mxxmaycgkyksb ky kb og
kzsoh nma pukqu k umxs ym hkjs nma ogz ym bss asohkbsz dcy rl
hmaz kn ky gsszb ds ky kb og kzsoh nma pukqu k or xasxoasz ym
zks
```

2. Let $\mathcal{E} = (Gen, Enc, Dec)$ be an encryption scheme. Prove:
   $\mathcal{E}$ is perfectly secret (a perfect cipher) $\iff$
   $\mathcal{E}$ is perfectly indistinguishable $\iff$
   $\mathcal{E}$ is adversarial indistinguishable

3. Let $p$ be a prime. Consider the following encryption scheme. The secret key is a pair $(a, b)$ sampled uniformly at random from $\mathbb{Z}_p^* \times \mathbb{Z}_p$. An encryption of a message $m \in \mathbb{Z}_p$ is defined as:
$$Enc_{a,b}(m) = a \cdot m + b \bmod p$$
   (a) Show that for any $b \in \mathbb{Z}_p$, if $u$ is distributed uniformly in $\mathbb{Z}_p$, then $b+u$ is also distributed uniformly in $\mathbb{Z}_p$. Show that for any $a \in \mathbb{Z}_p^*$, if $u$ is distributed uniformly in $\mathbb{Z}_p$, then $a \cdot u$ is also distributed uniformly in $\mathbb{Z}_p$.
   (b) Show that $Enc$ is perfectly indistinguishable.
   (c) Is it true that the encryptions of any two pairs of messages $(m_1, m_2)$ and $(m'_1, m'_2)$ have the same distribution, over a random choice of a secret key $(a, b)$, where the same secret key is used to encrypt both $m_1, m_2$ (or $m'_1, m'_2$)? Prove your claim.
   (d) What if we additionally assume $m_1 \neq m_2$ and $m'_1 \neq m'_2$? Prove your claim.
   (e) In this section we will implement the aforementioned encryption scheme using `SAGE`:
   - Choose a random prime $p$ in the range 2-10000
   - Sample uniformly at random a key $a \leftarrow \mathbb{Z}_p^*$ and $b \leftarrow \mathbb{Z}_p$
   - Implement a function $Enc(p, key, m)$ which gets a prime $p$, a key tuple $key = (a, b)$ and a message $m$ and encrypts the message
   - Implement a function $Dec(p, key, c)$ which gets a prime $p$, a key tuple $key = (a, b)$ and a ciphertext $c$ and decrypts the ciphertext. Note, in order to decrypt, we must find the inverse of $a$ modulo $p$ using the Extended GCD algorithm

   Useful `SAGE` functions:
   - `random_prime`
   - `randint`
   - `xgcd`

   Do not forget to submit your code.

4. Prove the following claim, stated in lecture 1, slide 24: For any encryption scheme, the number of ciphertexts must be at least as large as the number of plaintexts.

5. Prove Shannon theorem, stated in lecture 2, slide 6: A necessary condition for a perfect encryption scheme is that the number of keys is at least as large as the number of plaintexts messages (number of plaintexts messages with a-priori non-zero probability).

6. It is clear that if the key $k$ in the one-time pad scheme is the string of $\ell$ zeroes (i.e., $k = 0^\ell$), then the ciphertext equals the plaintext. That is, encryption does nothing. Due to this, it has been suggested that the one-time pad scheme be modified so that the key space $\mathcal{K}$ includes all strings of length $\ell$ except for $0^\ell$. Analyze the security of the modified scheme (with a formal proof), in particular, is it still perfectly secret?