Presentation for use with the textbook, Algorithm Design and Applications, by M. T. Goodrich and R. Tamassia, Wiley, 2015

Cryptography

Encryption

- Scenario:
  - Alice wants to send a message (plaintext p) to Bob.
  - The communication channel is insecure and can be eavesdropped If Alice and Bob have previously agreed on an encryption scheme (cipher), the message can be sent encrypted (ciphertext c)
- Issues:
  - What is a good encryption scheme?
  - What is the complexity of encrypting/decrypting?
  - What is the size of the ciphertext, relative to the plaintext?
  - If Alice and Bob have never interacted before, how can they agree on an encryption scheme?

Traditional Cryptography

- Ciphers were already studied in ancient times
- Caesar's cipher:
  - replace a with d
  - replace b with e
  - ...
  - replace z with c
- Caesar's cipher is an example of a monoalphabetic substitution cipher, which permutes the characters
- Armed with simple statistical knowledge, one can easily break a monoalphabetic substitution cipher
  - most frequent letters in English: e, t, o, a, n, i, ...
  - most frequent digrams: th, in, er, re, an, ...
  - most frequent trigrams: the, ing, and, ion, ...
- The first description of the frequency analysis attack appears in a book written in the 9th century by the Arab philosopher al-Kindi

Statistical Attacks

- Armed with statistical knowledge about the plaintext language, one can easily break a monoalphabetic substitution cipher
  - Most frequent characters in English: e, t, o, a, n, i, ...
  - Most frequent digrams: th, in, er, re, an, ...
  - Most frequent trigrams: the, ing, and, ion, ...
- The first description of the frequency analysis attack appears in a book written in the 9th century by the Arab philosopher al-Kindi
- Example (S. Singh, The Code Book, 1999):

  PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

  OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Frequency Analysis (1)

- We identify the most common characters, digrams and trigrams in the ciphertext
- Example

  PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

  OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

- First guess:
  - LBO is THE

Frequency Analysis (2)

- Assuming LBO represents THE, we replace L with T, B with H, and O with E and get

PCQ VMJYPD THYK TYSE KHXHJXWXV HXV ZCJPE EYPD KHXHJYUXJ THJEE KCPK. CP THE THCMKXPV XPV IYJKT PYDHT, QHEP KHO HXV EPVEV THE LXRE CI SX'XJMI, KHE JCKE XPV EYKKEV THE DJCMPV ZEICJE HYS, KXUYPD: "DJEXT EYPD, ICJ X THCMKXPV XPV CPE PYDHTK Y HXNE ZEEP JEACMPTYPD TC UCM THE IXZREK CI FXKT XDEK XPV THE REDEPVK CI XPAYEPT EYPDK. SXU Y SXEE KC ZCRV XK TC AJXNE X IXNCMJ CI UCMJ SXGEKTU?"

EFYRCDME, TXREK IJCS THE THCMKXPV XPV CPE PYDBTK

Decryption

- Code:

X	Z	A	V	O	I	D	B	Y	G	E	R	S	P	C	F	H	J	K	L	M	N	Q	T	U	W
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- Ciphertext:

  PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

  OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

- Plaintext:

  Now during this time Shahrazad had borne King Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: “Great King, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?”
  Epilogue, Tales from the Thousand and One Nights

Secret-Key Encryption

- A secret-key cipher uses a unique key K to encrypt and decrypt
- Caesar's generalized cipher uses the modular addition of each character (viewed as an integer) with the key:

$$C[i] = P[i] + K \bmod m$$

$$P[i] = C[i] - K \bmod m$$

- More secure secret-key encryption schemes have been devised in this century
- Examples:
  - DES
  - 3DES
  - IDEA
  - BLOWFISH
- With private-key encryption, a distinct secret key must be established for every pair of parties

Public-Key Encryption

- Bob uses a pair of keys (K_E, K_D) and
  - makes key K_E public
  - keeps key K_D private
- Anyone can use the public key K_E to encrypt a plaintext into a ciphertext sent to Bob
- Only Bob can decrypt the ciphertext using the private key K_D
- The most popular encryption scheme is RSA, named after its inventors Rivest, Shamir, and Adleman (1978)
- The RSA patent expired in 2000