Encyclopædia Iranica

CODES
Article by **Clifford Edmund Bosworth**

Published: December 15, 1992
Last Updated: November 20, 2013

CODES

CODES (*romūz*, sg. *ramz*), including the use of secret writing and cryptanalysis, in Persia. The use of codes in communications and diplomacy goes back to classical Greece, and an interest in codes and secret writing was carried into early Islamic times, not only for diplomatic purposes but also for magic and the concealment of trade secrets and esoteric religious views. Specific information for the Persian world is very sparse, but Ebn al-Nadīm (ed. Tajaddod, p. 16; tr. Dodge, pp. 25-26) mentioned two secret scripts said to have been used by the Sasanian kings. The *šāh-dabīrīya* was used for official correspondence and was forbidden to ordinary people. The *rāz-saharīya* was for secret messages to and from other countries. The Ghaznavid chancery of Sultan Masʿūd b. Maḥmūd made use of messages in code (*moʿammā, moʿammā-nāma*) in 423/1032 (Bayhaqī, ed. Fayyāż, pp. 403-04; tr. A. K. Arends, 2nd ed., Moscow, 1969, pp. 403-04). The most detailed available knowledge of the use of cryptography and cryptanalysis by medieval Islamic rulers comes from Qalqašandī's account of codes in the Mamluk sultanate of Egypt and Syria (pp. 229-51; cf. Bosworth). He explained that a message might be concealed through the use of invisible ink, an archaic or little-known alphabet, or a specially devised code. He also gave a number of examples of substitution ciphers, in which each character is substituted for another, and transposition ciphers, in which the order of the letters is changed. In several codes the *abjad* numerical values were used to represent letters. His system of code breaking was based on the structure and phonetic patterns of Arabic words.

It is likely that such codes were used by early Persian states as well, for nearly

identical versions were still in use in Qajar Persia. During the reigns of Fatḥ-ʿAlī Shah (1212-50/1797-1834) and Moḥammad Shah (1250-64/1834-48) the minister Abu'l-Qāsem Qāʾemmaqām devised a number of letter-substitution codes for communicating with different princes and viziers (Meftāḥ-al-Molk, 1902, pp. 22-23; Figure 77). The need for secure means of sending messages by telegraph and to foreign countries led to an increased interest in codes in the late 19th century (Meftāḥ-al-Molk, 1902, pp. 6-7). The first published Persian work on cryptography seems to have been *Ramz-e yūsofī* by the reformist diplomat Yūsof Khan Mostašār-al-Dawla.

A detailed account of Qajar cryptography and cryptanalysis can be found in the works of Mīrzā Moḥammad b. Yūsof, given the honorary title Meftāḥ-al-Molk by Nāṣer-al-Dīn Shah (1264-1313/1848-96) for his services to the state as an encoder and decipherer. His *Meftāḥ al-romūz* dealt with both ancient and contemporary codes, as well as some examples of his own devising (Figure 78). He identified two general types of code: letter-substitution ciphers (*ramz-e ḥorūfī*), in which the message is written with the aid of an alphabet table, and word-substitution ciphers (*ramz-e kalema*), in which a code book is used to replace each word with another, arbitrarily chosen word (Meftāḥ-al-Molk, 1909, pp. 8-9). Persian, Arabic, Turkish, and French letter-substitution and word-substitution codes were treated in separate chapters. The book includes a considerable number of old secret alphabets like the "tree script" (*qalam-e mošajjar*), *bornāvī*, "Hebrew," *ṭīrqāl*, and so on. The author divided modern codes into those devised before and those devised after the telegraph came into use. There are also instructions on deciphering codes based on letter frequency. Another work by Meftāḥ-al-Molk, *Nāseḵ al-romūz*, which has been reprinted several times, contains a system for encoding telegrams by means of a combination of word and letter substitution. This system proved to be deficient, however, as the arbitrary code groups were often garbled by the encoder or the telegraphers. He then wrote *Kašf al-asrār-e nāṣerī* in an attempt to remedy this problem by using whole words, usually proper nouns, to substitute for common words and phrases. The French equivalent for each code word made it possible to use the system abroad.

Aside from diplomatic communication, codes were used for religious and magical purposes in Persia, particularly among heterodox religious groups like the Ismailis and Ḥorūfīs. The Bābīs and Bahāʾīs used codes of various sorts for both security and pious purposes. Bābī manuscripts are often signed with numbers representing names. Personal names are often replaced by epithets

with identical numerical values. Finally, Mīrzā Moḥammad-ʿAlī, the second son of Bahāʾ-Allāh, devised the "Badīʿ script," which was used mostly for manuscript colophons (Āyatī, p. 189; cf. the colophons of two untitled collections of *alwāḥ* by Bahāʾ-Allāh, compiled in Bombay in 1890).

BIBLIOGRAPHY

ʿA.-H. Āyatī, *Kašf al-ḥīal* III, Tehran, 1326 Š./1957.

C. E. Bosworth, "The Section on Codes and Their Decipherment in Qalqashandi's *Ṣubḥ al-aʿshā*," *Journal of Semitic Studies* 8, 1963, pp. 17-33; repr. *in Medieval Arabic Culture and Administration*, London, 1982, no. XIII.

D. Kahn, *The Codebreakers*, New York and London, 1967 (a good general work on codes and the history of their use).

Mīrzā Maḥmūd b. Yūsof Meftāḥ-al-Molk, *Ketāb-e nāseḵ al-romūz wa ramz-e maḥmūdī*, Tehran, 1299/1882.

Idem, *Kašf al-asrār-e nāṣerī*, Tehran, 1313/1895.

Idem, *Meftāḥ al-romūz*, Tehran, 1320/1902 (for a review of all three works, see C. Huart, *JA*, ser. 10/9, 1907, pp. 360-62).

Mostašār-al-Dawla, *Ramz-e yūsofī*, Tehran, 1282/1865.

Qalqašandī, *Ṣobḥ al-aʿšā*, ed. M.-ʿA. Ebrāhīm, IX, Cairo, 1340/1922.

Figure 77. A letter-substitution code used by Qāʾemmaqām. After Meftāḥ-al--Molk, 1320/1902, p. 29.

Figure 78. The "Greek script," a traditional Persian code. After Meftāḥ-al-Molk, 1320/1902, p. 13.