



现代密码学

第二讲 中国古代密码艺术

信息与软件工程学院



第二讲 中国古代密码艺术



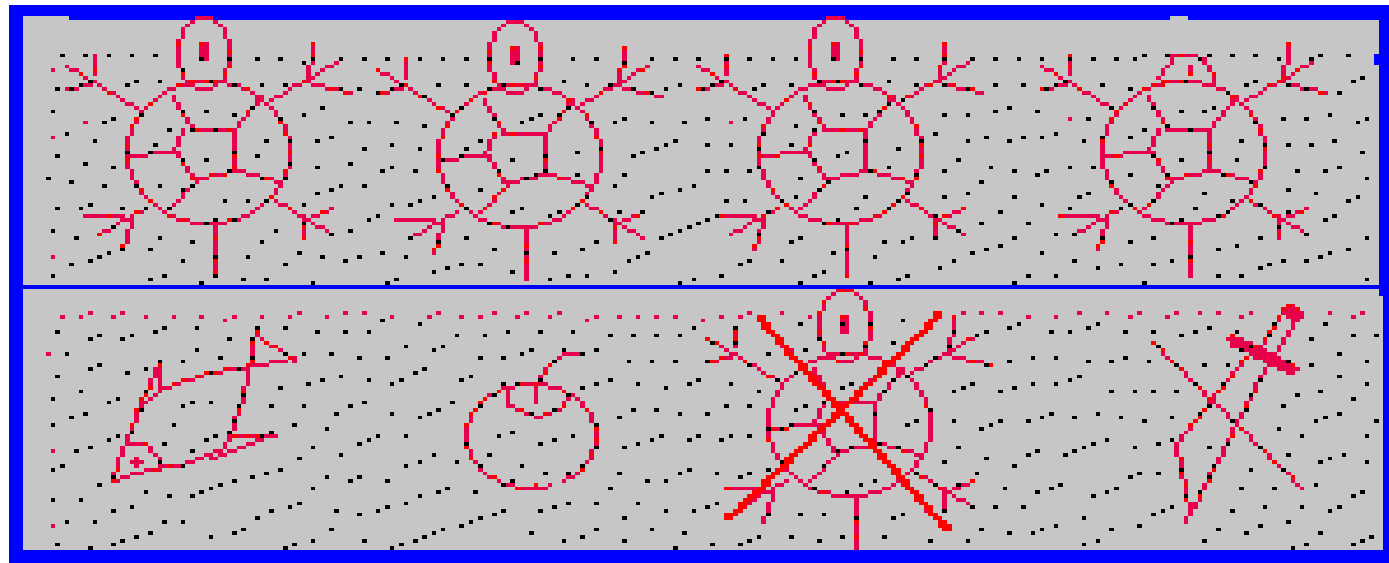
中国民间艺术

中国古代军事密码

中国近代密码

图画传情

- 古代留守在家中的妻子给外出工作的丈夫的书信



归，归，归！速归！如果（鱼果）不归，一刀两断

会意诗




长夜横枕意心歪，
月斜三更门半开，
短命到今无口信，
肝肠望断无人来。

A decorative element consisting of several horizontal blue bars of varying lengths, stacked vertically, is positioned to the left of the title.

藏头诗

- 将秘密消息隐藏在其他消息中

A red rectangular box highlights the first character of each line of the poem, which are '我', '爱', '秋', and '香', forming the hidden message '我爱秋香' (I love autumn fragrance).

我画蓝江水悠悠，
爱晚亭上枫叶愁。
秋月溶溶照佛寺，
香烟袅袅绕经楼。

A decorative graphic consisting of several horizontal blue bars of varying lengths, stacked vertically, is positioned to the left of the section header.

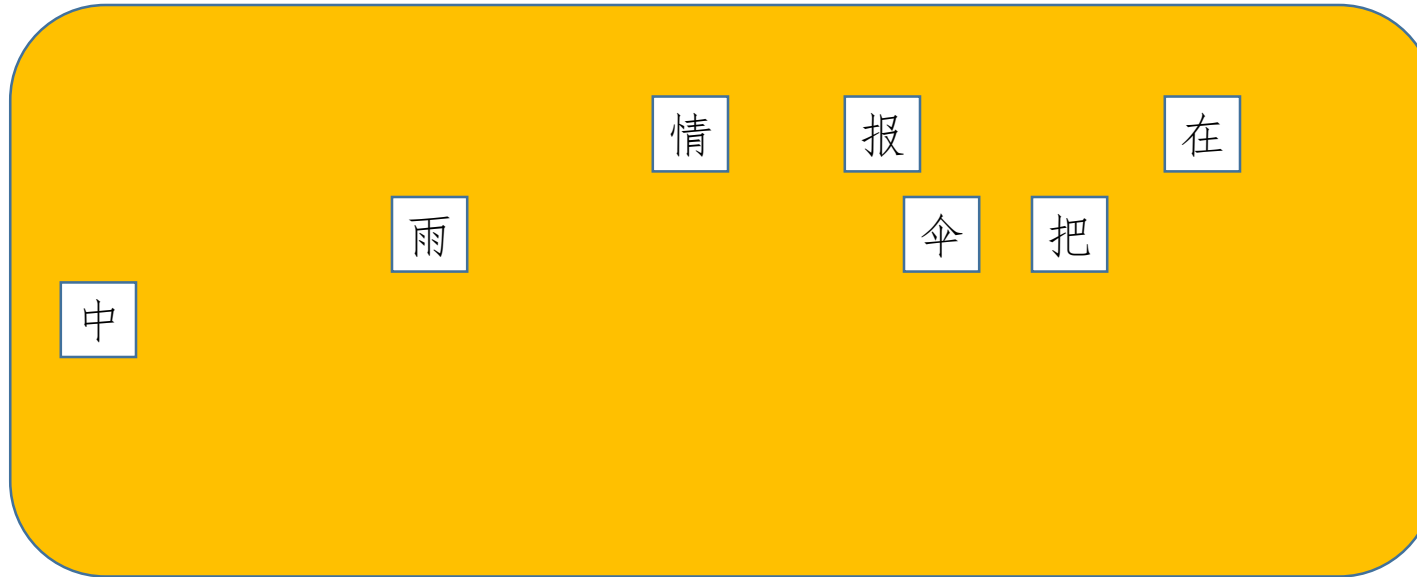
叠痕法

- 先把信纸折叠几下（上下及左右），然后铺平信纸
 - 将传递的信息按顺序一个个分开，写在折痕的交叉点上，每一个交叉点写一个字
 - 在空白位置上填上公开的普通信文，普通信文与秘密信文的文字通顺地连贯在一起
 - 为了防止被敌人察觉，使用这种密码需要在编公开信文上下些功夫。如果在秘密信文上再用些暗语式密码，那么敌人就更难看出破绽了。
-

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

漏格板加密法

例：密文：



明文：情报在雨伞把中。



第二讲 中国古代密码艺术



中国民间艺术

中国古代军事密码

中国近代密码

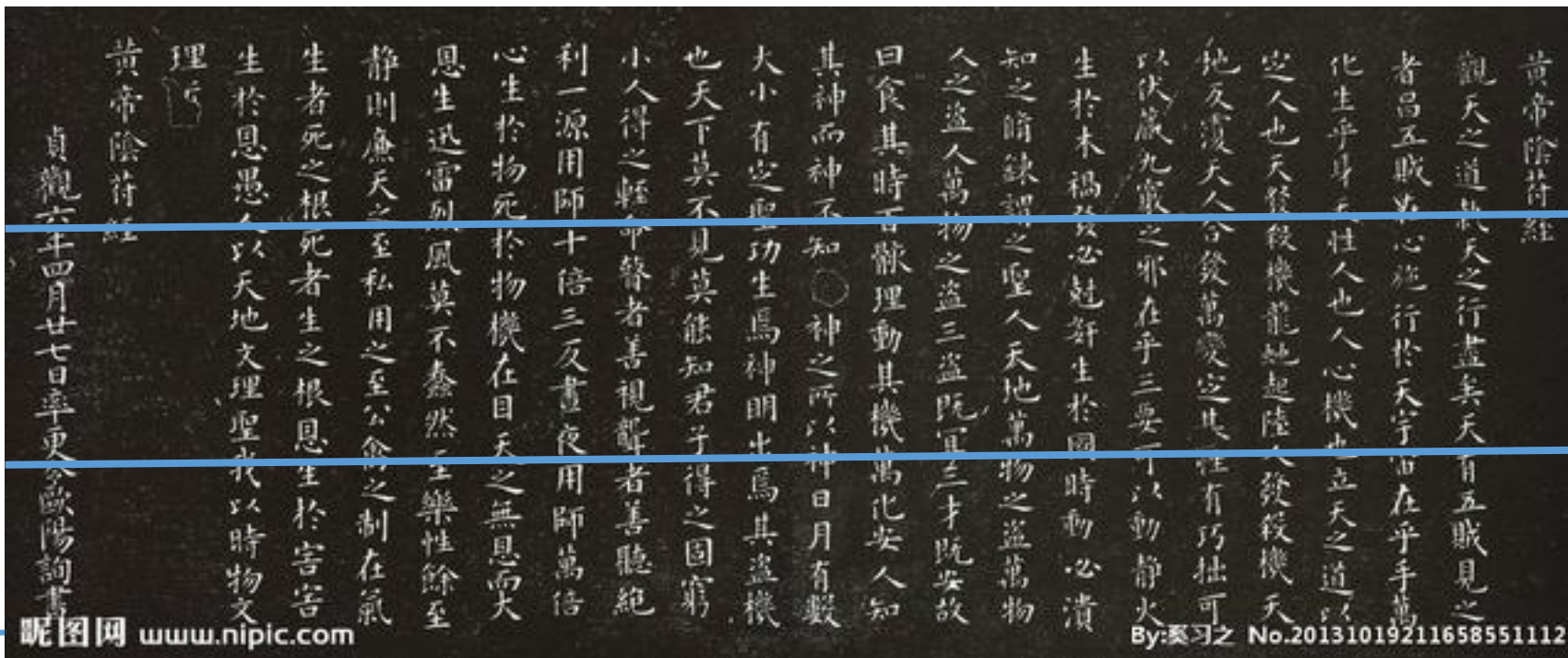
阴符（〈六韬·龙韬·阴符〉）

- 武王问太公曰：‘引兵深入诸侯之地，三军猝有缓急，或利或害。吾将以近通远，从中应外，以给三军之用。为之奈何？’
太公曰：‘主与将，有阴符。凡八等：
 - 大胜克敌之符，长一尺；破军擒将之符，长九寸；
降城得邑之符，长八寸；却敌报远之符，长七寸；
警众坚守之符，长六寸；请粮益兵之符，长五寸；
败军亡将之符，长四寸；失利亡士之符，长三寸。
- 八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫之通识。’

阴书（〈六韬·龙韬·阴书〉）

创造者：相传也是由姜子牙发明

用法：把一封竖写的秘密文书横截成3段，派出3个人各执一段，于不同时间、不同路线分别出发，先后送给收件者。收件者收齐了3段文件才能悉知秘密文书的全部内容。万一送件途中某一发送者被敌方截获，敌方也难以解读文书的全部内容。





中国古代军事密码

- 北宋《武经总要》
- 曾公亮
- 军队中常用的40种战斗情况

1请弓	2请箭	3请刀	4请甲	5请枪旗	6请锅幕	7请马	8请衣赐	9请粮料	10请草料
11请车牛	12请船	13请攻城 守具	14请添兵	15请移营	16请进军	17请退军	18请固守	19未见贼	20见贼讫
21贼多	22贼少	23贼相敌	24贼添兵	25贼移营	26贼进兵	27贼退兵	28贼固守	29围得贼城	30解围城
31被贼围	32贼围解	33战不胜	34战大胜	35战大捷	36将士投降	37将士叛	38士卒病	39都将病	40战小胜

中国古代军事密码（续）

- 这套密码的使用方法是：
 - 约定一首40字的五言律诗
 - 保密，文字不得重复
- 假设双方以唐代王勃的《送杜少府之任蜀川》
 - 城阙辅三秦，风烟望五津。
 - 与君离别意，同是宦游人。
 - 海内存知己，天涯若比邻。
 - 无为在歧路，儿女共沾巾。

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

中国古代军事密码（续）

- 如果军队在战斗在粮食将尽，需要补充，前方将领就从密码本中查出“请粮料”的编码，是第九，而《送杜少府之任蜀川》中的第九字是“五”。于是请粮将领就将“五”字写到一件普通公文书牒之中，并在字上加盖印章。
- 指挥机关接到这件公文后，查出盖印章的“五”字，得知“五”字在临时约好的诗中列第九，再对照密码本上的顺序，就得知了前方的情报。

反切码

- 原理：使用汉字的“反切”注音方法进行编码
- 发明人是著名的抗倭将领戚继光。
- **密钥**：“柳边求气低，波他争日时。莺蒙语出喜，打掌与君知。”“春花香，秋山开，嘉宾欢歌须金杯，孤灯光辉烧银缸。之东郊，过西桥，鸡声催初天，奇梅歪遮沟。”
- **加密方法**：前一首诗歌的前15个字作为声母，依次编号为1-15；后一首诗歌的36字为韵母，按顺序编号为1-36；然后再将当时字音的八种声调，也按顺序编号为1-8，就编写出完整的“反切码”体系。
- 例如：如果密码的编号是“5-25-2”，5是声母“低”字，25是韵母“西”字，2是声调的二声。据此，“5-25-2”就可以读为“敌”字。



第二讲 中国古代密码艺术



中国民间艺术

中国古代军事密码

中国近代密码

中国近代密码

- 密本型：用预先编定的字母或数字密码组，代替明文中的数字、字母、音节、单字、词汇、短语、符号等，以实现明密变换。
- 汉字6899个，按部首笔画为序排列，以四码数字与其相匹配
- 明文： 三 人 之 中
- 明码：0005 0086 0037 0022
- 密文：7970 7947 7966 7981
- 在普通本基础上，密本里编制词汇、短语、句子等，既增加密本的密度，又缩短电报长度，称作“特别本”。

A decorative blue horizontal bar with a series of horizontal lines is positioned to the left of the title.

中国近代密码

- 加乱型：用有限元素(字母或数码)组成的一串序列作为乱数，按规定的算法，与明文信息序列相结合变成密信息。如：
 - 明码： 中 国 人 民
 - 0022 0948 0086 3046
 - 乱数： 2901 4561 8265 7039
 - 密文： 2923 4409 8241 0075
 - $C1(\text{密}) = M1(\text{明}) + K1(\text{乱}) \pmod{10}$
 - $M1(\text{明}) = C1(\text{密}) - K1(\text{乱}) \pmod{10}$
-



感谢聆听!

xynie@uestc.edu.cn