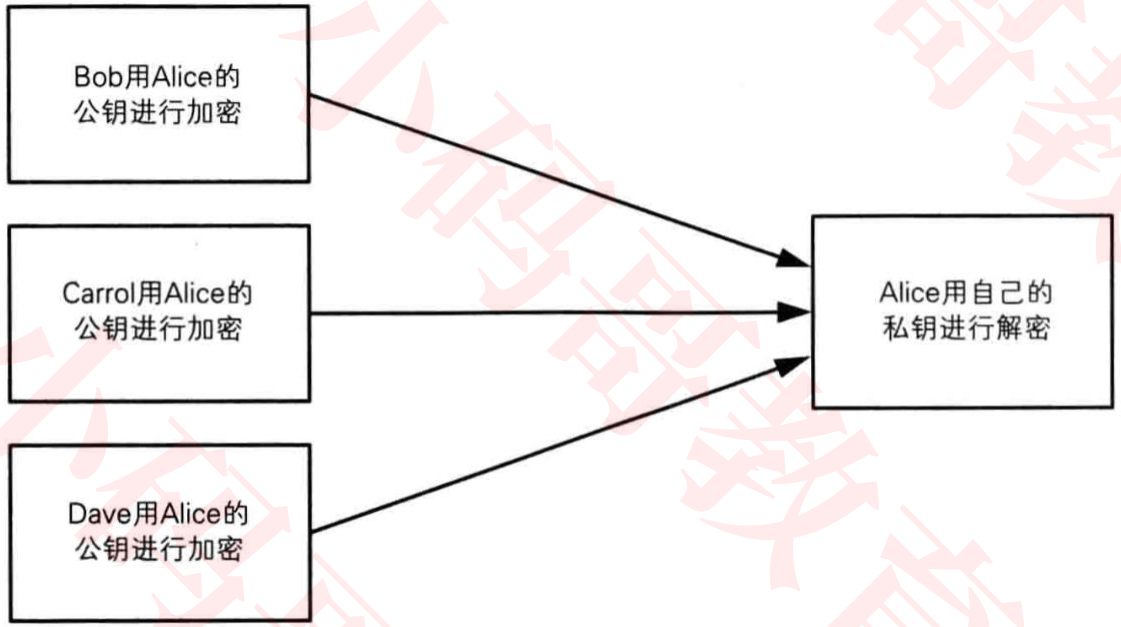
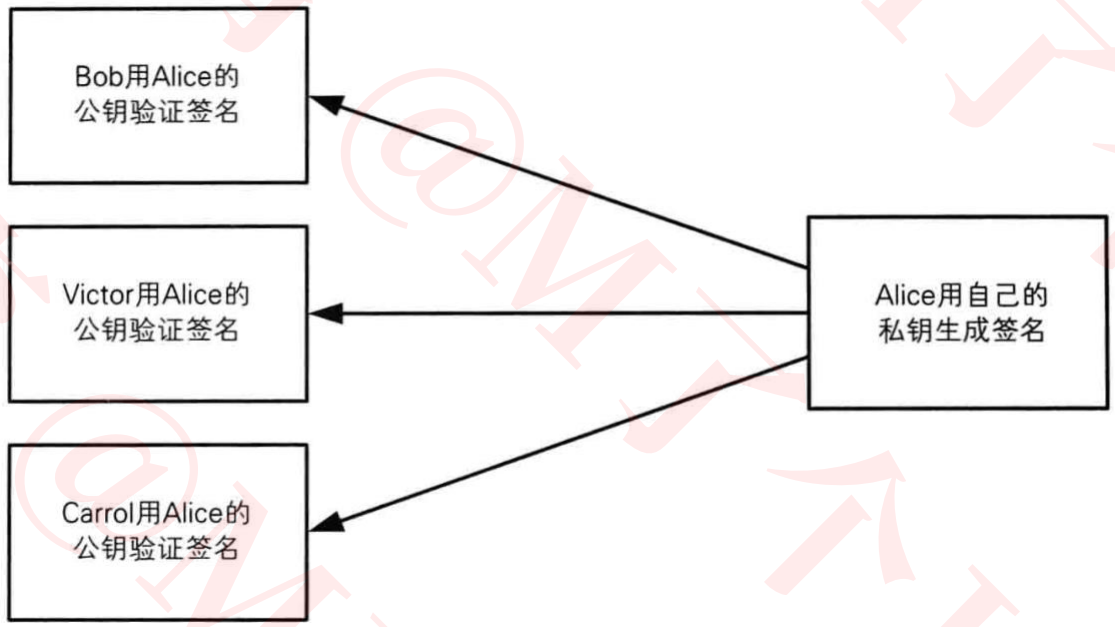
非对称加密 – 公钥、私钥再总结



在**非对称加密**中，任何人都可以使用公钥进行加密



在**数字签名**中，任何人都可以使用公钥验证签名

非对称加密 – 公钥、私钥再总结

- **数字签名**，其实就是将**非对称加密**反过来使用

	公钥	私钥
非对称加密	发送者加密时使用	接收者解密时使用
数字签名	验证者验证签名时使用	签名者生成签名时使用
谁持有密钥?	只要有需要，任何人都可以持有	个人持有

- 既然是加密，那肯定是不希望别人知道我的消息，所以只有我才能解密
  - **公钥**负责加密，**私钥**负责解密

- 既然是签名，那肯定是不希望有人冒充我发消息，所以只有我才能签名
  - **私钥**负责签名，**公钥**负责验签