

Dissecting Pretty Good Privacy (PGP)

Dr. Craig A. Rich
Computer Science Department
Cal Poly Pomona

www.csupomona.edu/~carich/biography/dissecting_pgp.pdf

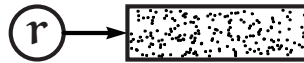
Security Primitives

- Random Number Generator
- Symmetric Cipher
- Asymmetric Cipher
- Hash Function
- Compression Function

Pretty Good Privacy (PGP)

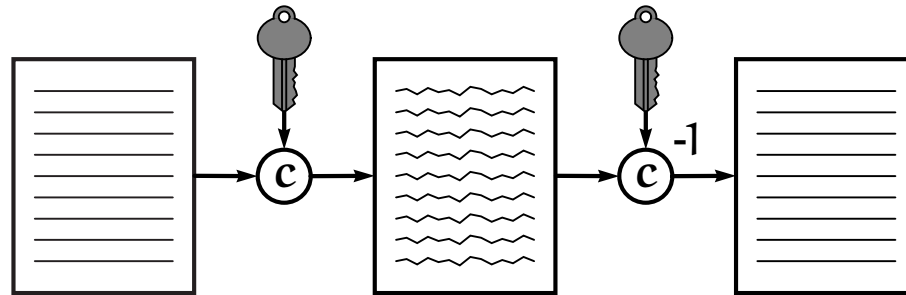
- Dissecting PGP
- Chains of Trust

Random Number Generator (RNG)



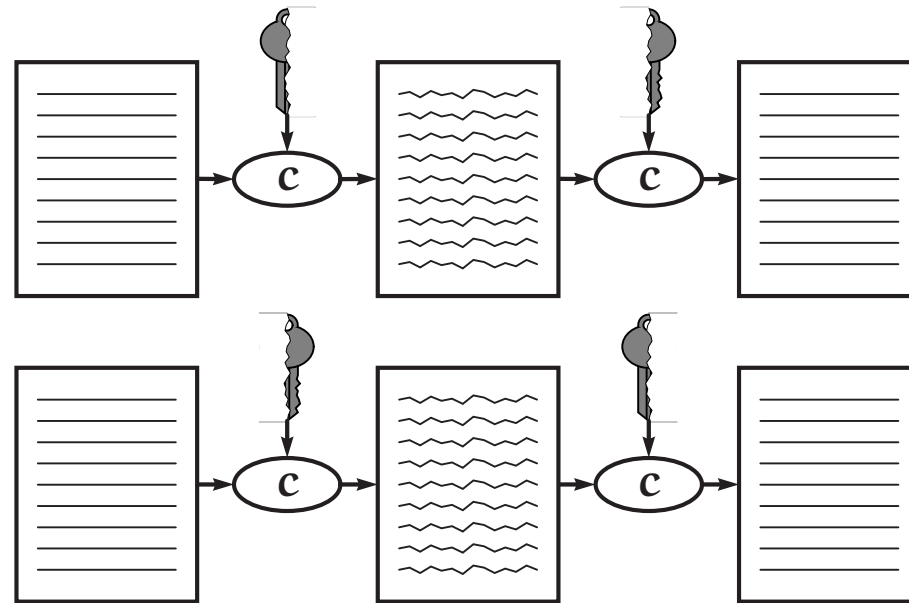
- should produce uniformly random bits
- e.g. r = hardware RNG,
 r = software pseudo-RNG (PRNG) based on a seed

Symmetric (Secret Key) Cipher



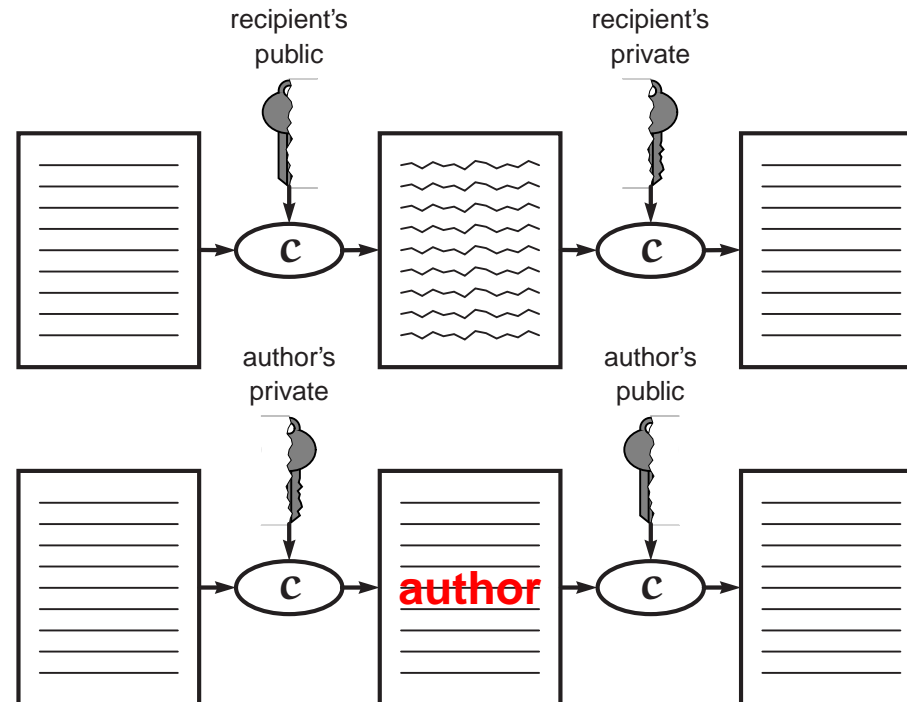
- assume enemy knows ciphertext and ciphers c , c^{-1}
- producing plaintext or secret key should be intractable
- secrecy requires long random secret key
- e.g. $c = \text{AES, 3DES, IDEA, CAST5, Blowfish} \dots$ run in linear time

Asymmetric (Public Key) Cipher



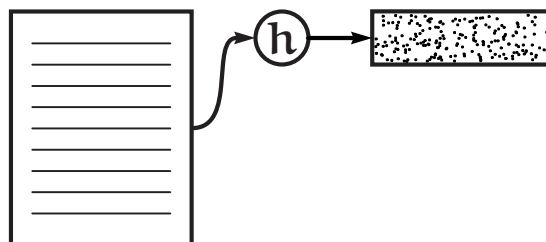
- users generate their own key pairs
- assume enemy knows ciphertext and cipher c
- producing plaintext or either key should be intractable
- producing one key from the other key should be intractable
- e.g. $c = \text{RSA, ElGamal, DSA} \dots$ run in superlinear time

Asymmetric (Public Key) Cipher



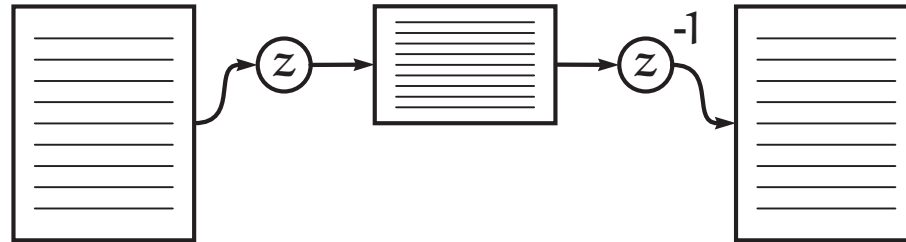
- users publish a **public key**, keep secret a **private key**
- encrypt using recipient's public key, decrypt using recipient's private key
- sign using author's private key, verify using author's public key

Hash Function



- hash function h outputs short fixed-length (e.g. 128-bit) hashes
- assume enemy knows hash and hash function h
- producing distinct plaintexts mapping to one hash should be intractable
- e.g. $h = \text{SHA1, MD5, RIPEMD160, SHA256} \dots$ run in linear time

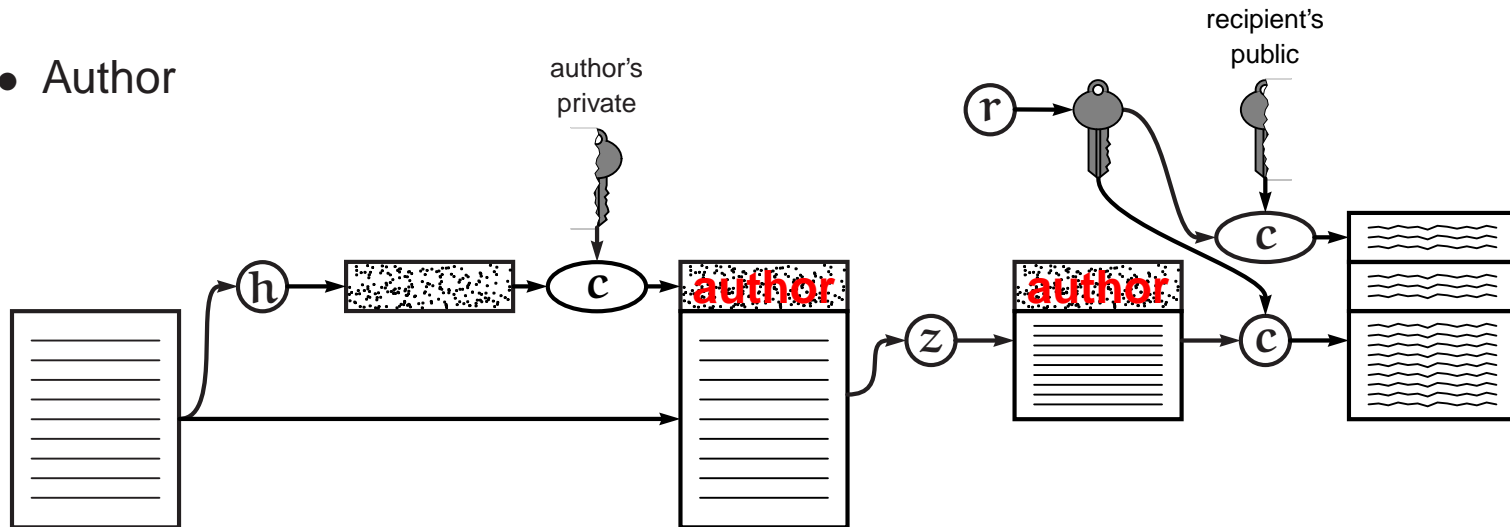
Compression Function



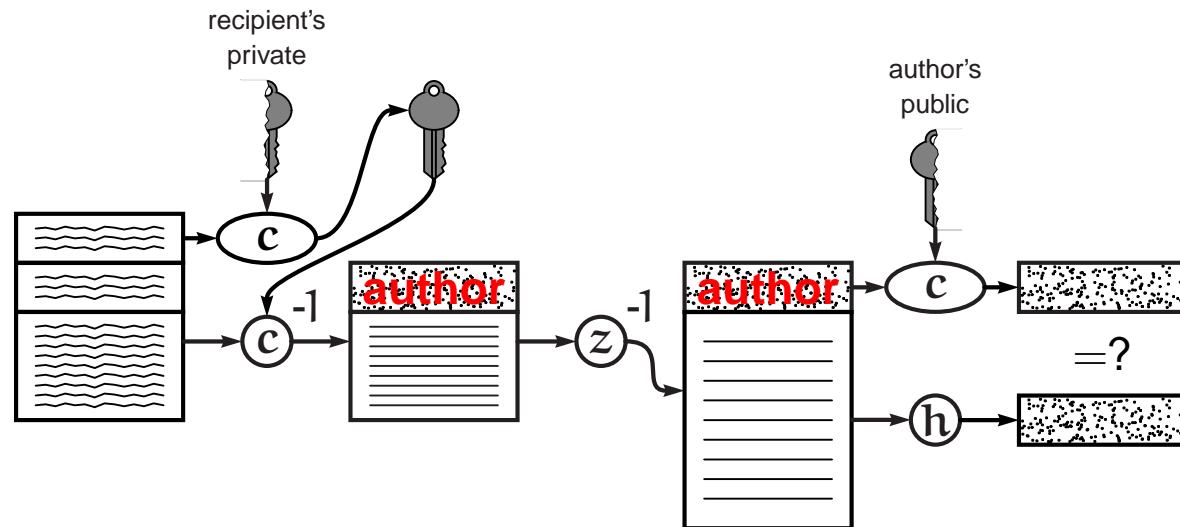
- degree of compression depends on redundancy (lack of entropy)
- compression increases entropy
- e.g. $z = \text{ZIP, ZLIB, BZIP2} \dots$ run in linear time

Dissecting PGP

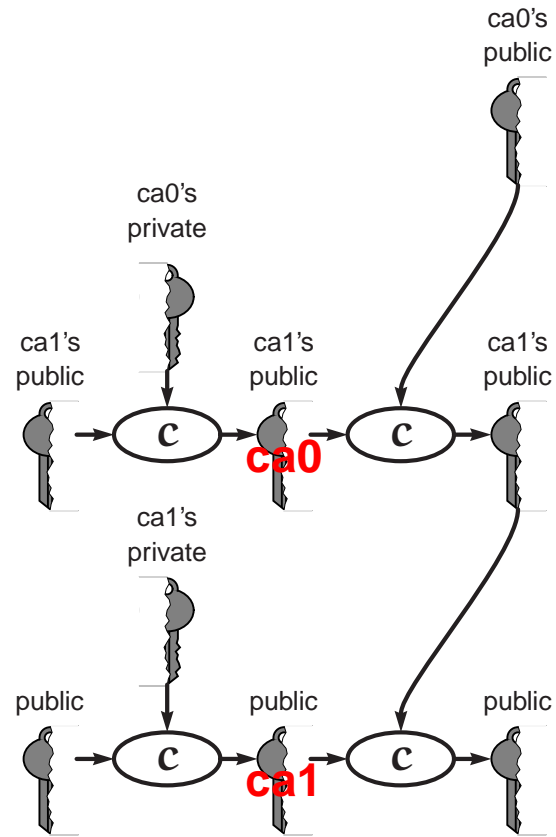
- Author



- Recipient



Chains of Trust



- a **certificate** is a public key signed by a **certificate authority**