An Explanation of Cryptographic Key Fingerprint Visualization Technology

Joe Awni

joe.awni@gmail.com

Outline

What is Cryptography?

- Etymologically : from Greek , "hidden writing"
- The practice and study of secure communication

What is Asymmetric Cryptography (AC)?

AC refers to algorithms capable of using two different keys for encryption and decryption. Because the keys share mathematical relation, they are referred to as asymmetrical.
(i.e.: One key is used to encrypt the message and only a second key may decipher)

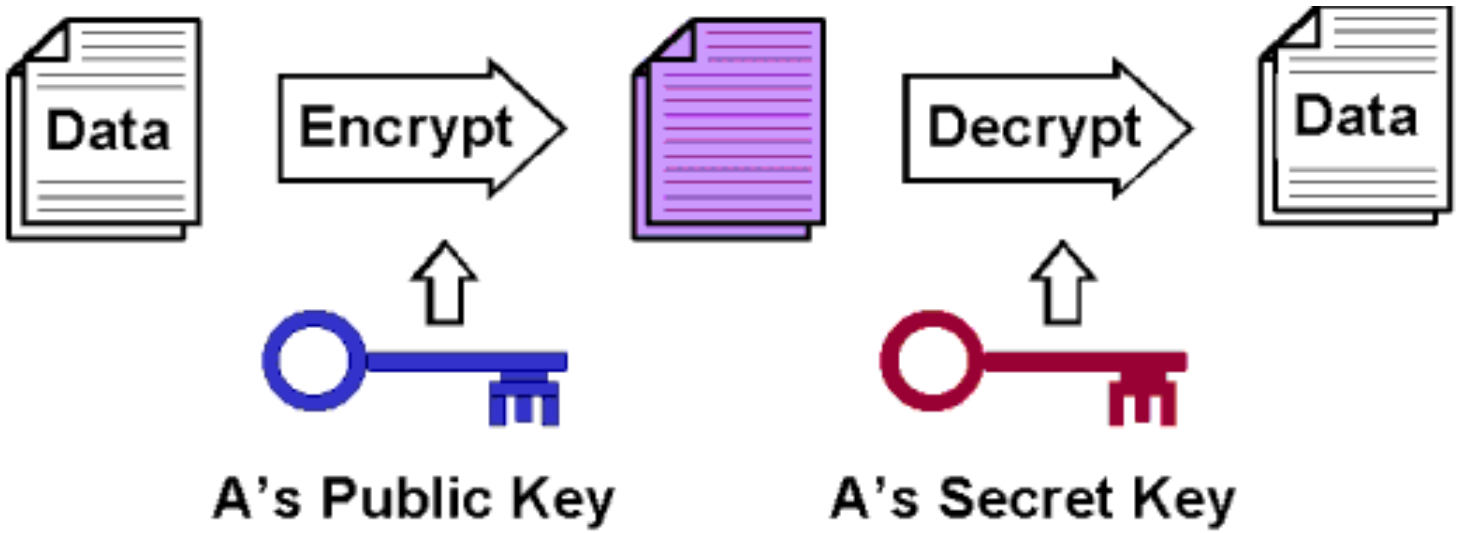


Figure: The purple icon represents the cipher-text.

Why is Asymmetric Cryptography widely known as Public-key Cryptography?

- Although the distinction is arbitrary, users of PGP/GPG Software keep one key private, and disseminate a second, public key.
- PGP/GPG software is not nearly the most widely used format of asymmetric key algorithm technology; HTTPS is. Thus, it does not make sense to refer to this field of cryptography as public-key.
- Frankly, key-pair cryptography would be the most straight-forward name.

Why is Asymmetric Cryptography important?

- Encrypted messages may be exchanged without prior arrangement on an encryption algorithm and key.
- Thus, this technology is widely used on the World Wide Web (WWW).
- You are already using it, whether-or-not you know it.

How does it work?

- Randomly chosen large prime numbers are used to generate two keys that protect the clear-text message with a computational barrier. Without the encryption key's pair, it would take an extremely long time to decipher the clear-text.

$$p, q$$
$$n = pq \qquad \phi(n) = (p-1)(q-1)$$
$$e, \qquad 1 < e < \phi(n) \qquad \gcd\big(e, \phi(n)\big) = 1$$
$$d = e^{-1} \bmod \phi(n)$$

Figure: RSA key generation algorithm

What is the vulnerability?

- Since asymmetric cryptography makes it easy to set up encrypted two-party communication without prior arrangement on an algorithm and key, the challenge is identifying the remote party.
- Basically, to set up encryption "on the fly" is no problem, but knowing who you are "talking" to is a fundamental issue with modern cryptosystems.

What is a key fingerprint?

- A cryptographic hash of a key
- An example in typical hexadecimal format:
  - 1f:0d:00:0c:bd:ba:cb:a0:39:75:ee:91:7d:16:d1:fe

What is a Cryptographic hash?

- Also known as digest
- Takes arbitrary data and returns a fixed-size bit string such that
  - It is infeasible to generate a message given a hash (one directional)
  - It is infeasible to modify the message without changing the hash

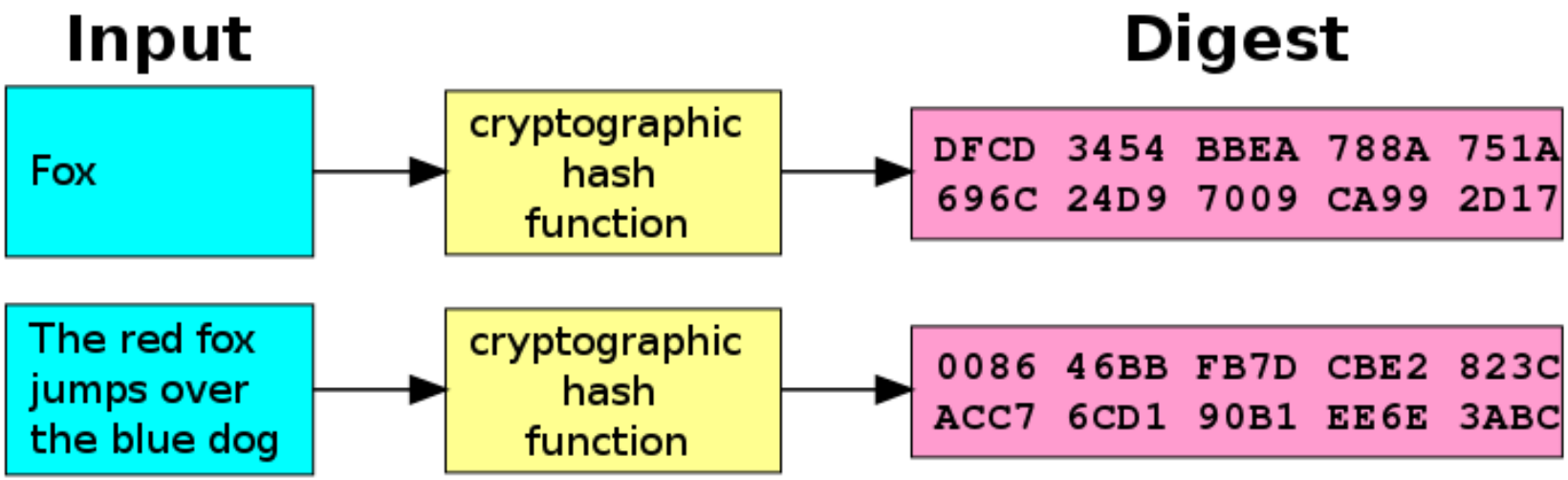


Figure: Cryptographic Hash Function Flow Chart

What is the significance of a key fingerprint?

- Basically, it addresses the issue of, "who am I talking to."
- A key fingerprint, generated from an encryption key, and compared to a known value can be used to authenticate a remote party.
- Note: It is important to generate the fingerprint on your computer from the remote party's encryption key, rather than rely on a third party for authentication.

Common uses:

- SSL (includes all https:// sites)
- S/MIME (encrypted email)
- PGP / GPG (encrypted email)
- SSH (secure terminal)
- SFTP (secure file transfer)

Secure Sockets Layer (SSL)

Trusted CAs (Certificate Authorities) cryptographically sign key fingerprints to produce certificates used to identify web servers.

- The most widely used form of asymmetric encryption
- Remote hosts are reached by unencrypted DNS entries
- Third party CAs are used to authenticate the remote host
  - Public Key Infrastructure (PKI)

Secure Shell (SSH)

User is asked to positively identify the remote party by comparing a key fingerprint to a known value

- Asks user to authenticate remote host by key fingerprint
- If you ever used SSH before you are familiar with :

```
The authenticity of host '[target.net]:23
([69.141.191.69]:226)' can't be established.
ECDSA key fingerprint is
 1f:0d:00:0c:bd:ba:cb:a0:39:75:ee:91:7d:16:d1:fe.
Are you sure you want to continue connecting (yes/no)?
```

GNU Privacy Guard / Pretty Good Privacy (GPG / PGP)

Users can chooses to trust others, and trust others to identify/introduce others.

- Relies on key fingerprints and
- Web of Trust (https://en.wikipedia.org/wiki/Web_of_trust)
  - Decentralized alternative to PKI
  - Basically extends some cryptographic authenticity to "friends of friends"

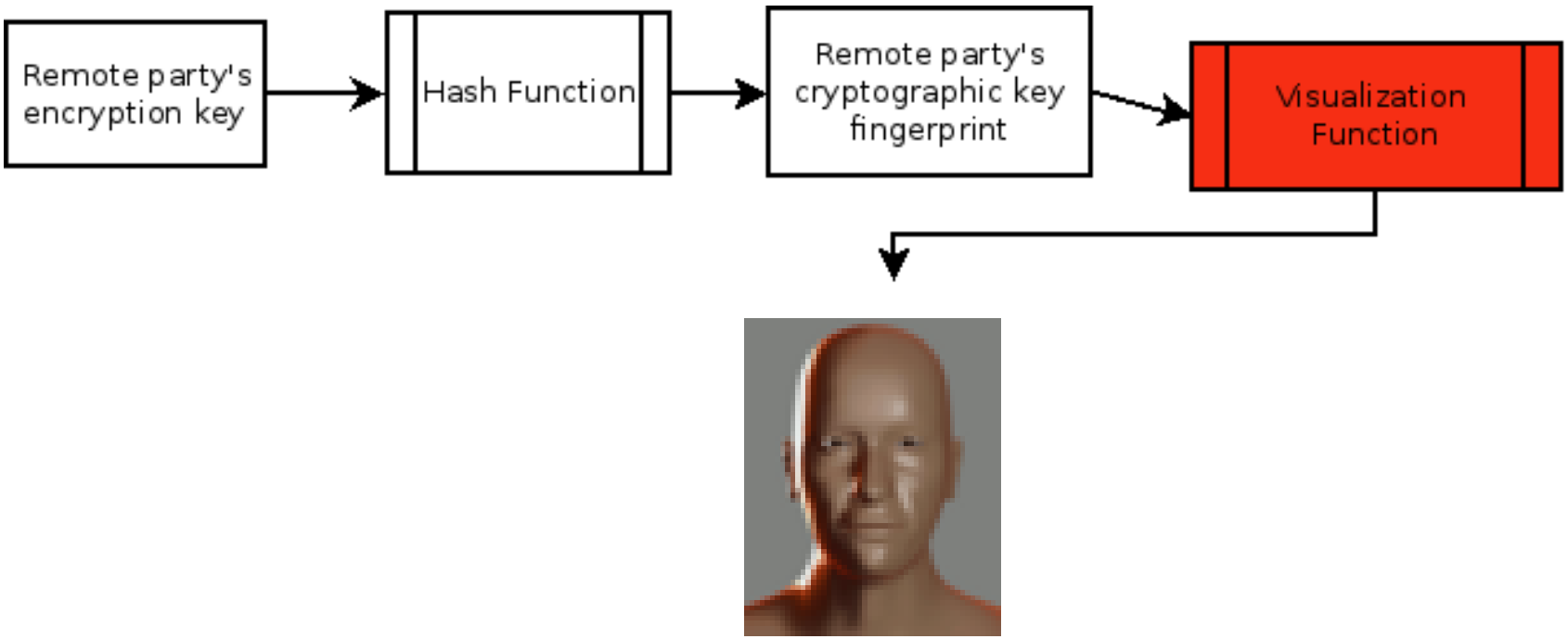
Strengths and Weakness of Modern Cryptosystems

Choosing a decentralized model for future technologies of the WWW is of strategic importance. Just as mission critical facilities have generators to restore power in the event of a black-out, the WWW should have no single point of failure.

- Web browsers use of PKI (centralized system) should be balanced by incorporating a fault-tolerant distributed system.

Visualization Uses

- Rather than require users to memorize key fingerprints to identify remote parties or identification authorities, a memorable visualization can be used to aid PKI, Web of Trust, or any encryption technology. Visualizing key fingerprint means authentication can be as simple as asking a user, do you remember this face?"



Full Size Face Visualization