University of Basel
Center for Innovative Finance

Bitcoin, Blockchain and Cryptoassets
Asymmetric Cryptography

Prof. Dr. Fabian Schär
University of Basel

Release Ver.: (Local Release)
Version Hash: (None)
Version Date: (None)

Diffie-Hellman-Merkle Key Exchange

- Whitfield Diffie, Martin Hellman and Ralph Merkle find a solution for the *key distribution* problem (1976)
- They still use symmetric encryption. However, the key can be generated securely on a potentially compromised channel.

- Alice and Bob define ex-ante
  - One-way function: $G^x \ (mod\ P)$
  - Parameters: $G = 7$ and $P = 11$

Diffie-Hellman-Merkle Key Exchange

	Alice	Bob
Step 1	chooses $A = 3$	chooses $B = 6$
Step 2	$\alpha = G^A \ (mod\ P)$ $\alpha = 7^3 \ (mod\ 11) = 2$	$\beta = G^B \ (mod\ P)$ $\beta = 7^6 \ (mod\ 11) = 4$
Step 3	Alice sends her result $\alpha = 2$ to Bob	Bob sends his result $\beta = 4$ to Alice
Exchange	*They exchange α and β (not A and B!)*	
Step 4	Alice computes $k = \beta^A \ (mod\ P)$ $k = 4^3 \ (mod\ 11) = 64 \ (mod\ 11) = 9$	Bob computes $k = \alpha^B \ (mod\ P)$ $k = 2^6 \ (mod\ 11) = 64 \ (mod\ 11) = 9$
Key	*Alice and Bob have agreed on key $k = 9$, because:* $\alpha^B \ (mod\ P) = G^{AB} \ (mod\ P) = G^{BA} \ (mod\ P) = \beta^A \ (mod\ P)$	

Table: Diffie-Hellman-Merkle-Key-Exchange. Based on [2]

Issues

Interactive process may be cumbersome.

- Synchronous communication to establish key
- Separate setup for each peer

Asymmetric Cryptography

- So far: Symmetric cryptography
  - Decryption is inverse algorithm of encryption
- Diffie's Idea (1975): Asymmetric encryption
  - Key to encrypt and key to decrypt a message are not identical
- ...but how?

Asymmetric Cryptography

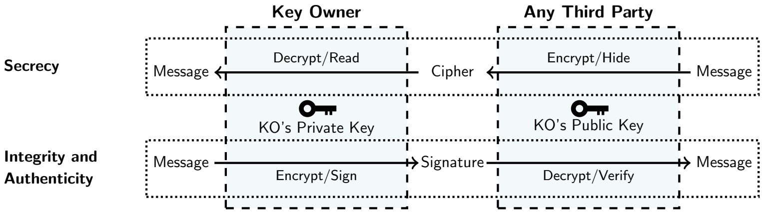
- Ronald Rivest, Adi Shamir and Leonard Adleman
- Inspired by Diffie's idea of asymmetric cryptography
- Develop first asymmetric encryption algorithm (*RSA*) [1]

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

RSA

Properties of asymmetric cryptography:



RSA 1/4: Find Public Key

Alice chooses two primes p and q (e.g., $p = 17$ and $q = 11$) and computes

$$N = p \cdot q$$

In our example:

$$N = 17 \cdot 11 = 187$$

and choose an additional integer e (e.g., $e = 7$).[1]

$\Rightarrow$ N and e together make up the public key which Alice can make publicly available.

[1] e and $(p-1) \cdot (q-1)$ must be relatively prime, i.e. not share any factors other than 1.

RSA 2/4: Encrypt Message

Bob encodes message M as an integer (e.g., letter X in ASCII $= 88$) and computes the encrypted message C using Alice's public key and the message:

$$C = M^e \ (mod \ N)$$

In our example:

$$C = 88^7 \ (mod \ 187)$$
$$C = 11$$

RSA 3/4: Derive Private Key

Alice computes private key k_p using:

$$e \cdot k_p = 1 \ (mod \ \phi(N)) \text{ , where } \phi(N) = (p-1)(q-1)$$

In our example:

$$\begin{aligned} 7 \cdot k_p &= 1 \ (mod \ 16 \cdot 10) = 1 \ (mod \ 160) \\ k_p &= 23 \end{aligned}$$

Note: Extended Euclidean algorithm is needed for this step

RSA 4/4: Decrypt Message

Alice decrypts Bob's message with:

$$M = C^{k_p} \ (mod\ N)$$

and computes

$$M = 11^{23} \ (mod\ 187)$$
$$M = 88 = X \text{ in ASCII}$$

RSA: Requirements

Crucial:

- N has to be sufficiently large
- It has to be impossible to find p and q by using prime factorization of N.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM **21** (1978), no. 2, 120–126.

[2] Simon Singh, *The Code Book: The Secret History of Codes and Codebreaking*, Fourth Estate London, 1999.