Introduction to Cryptocurrency

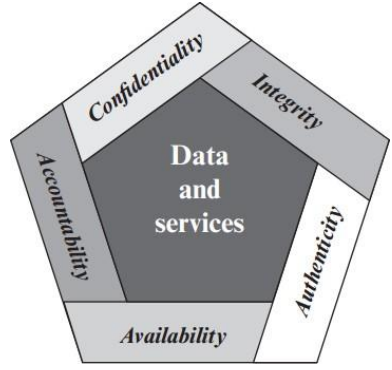
Symmetric Cryptosystems

CIA TRIAD

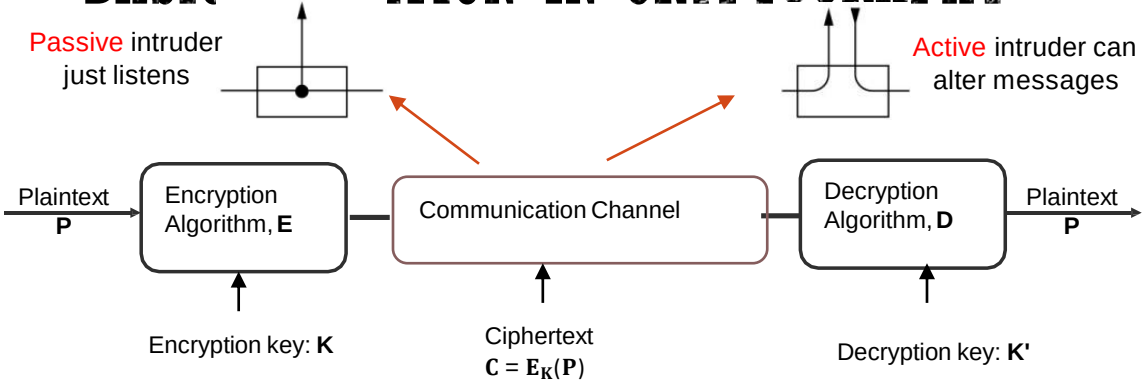
- **Confidentiality:** Preserving authorized restrictions on information access and disclosure.
  - A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction.
  - A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to information.
  - A loss of availability is the disruption of access to or use of information or an information system.

OTHER SECURITY REQUIREMENTS

- **Authenticity:** The property of being genuine and being able to be verified and trusted.
  - This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - We must be able to trace a security breach to a responsible party.
  - Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

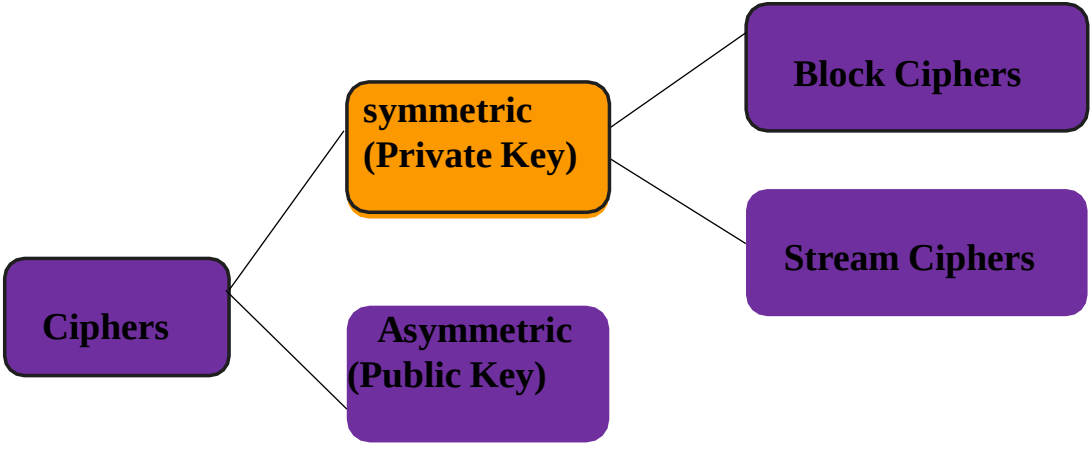


BASIC SITUATION IN CRYPTOGRAPHY



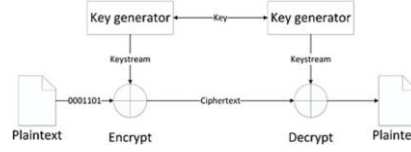
- **Passive attack**: the attacker only monitors the traffic attacking the confidentiality of the data
- **Active attack**: the adversary attempts to alter the transmission attacking data integrity, confidentiality, and authentication, system resources or affect their operations

CLASSIFICATION OF CRYPTOSYSTEMS

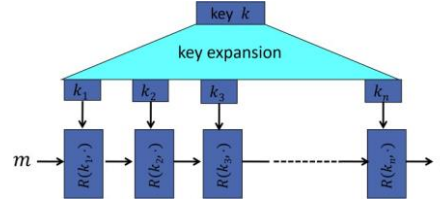


SYMMETRIC CIPHERS

- **Stream cipher** is one that encrypts a digital data stream one bit (or byte) at a time
  - Example: autokey Vigenère system



- **Block cipher** is one in which the plaintext is divided in blocks and one block is encrypted at one time producing a ciphertext of equal length
  - 64 bits or 128 bits are typical block lengths
  - Many modern ciphers are block ciphers



ADVANCED ENCRYPTION STANDARD

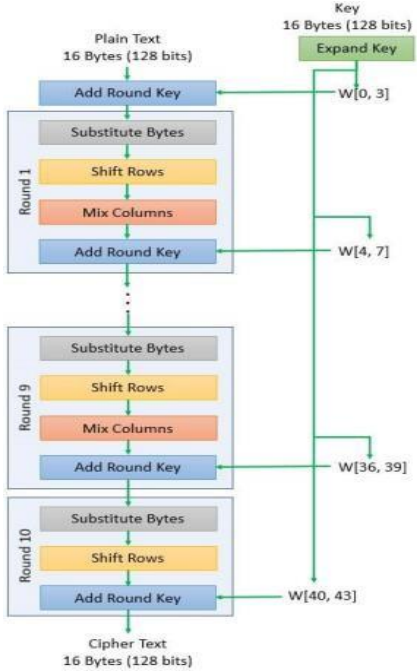
- AES competition
  - Started in January 1997 by NIST
  - 4-year cooperation between
  - U.S. Government
  - Private Industry
  - Academia

- Why?
  - Replace 3DES
  - Provide a publicly disclosed encryption algorithm, available royalty-free, worldwide

THE FINALISTS

- **MARS**
  - IBM
- **RC6**
  - RSA Laboratories
- **Rijndael**
  - Joan Daemen (Proton World International) and Vincent Rijmen (Katholieke Universiteit Leuven)
- **Serpent**
  - Ross Anderson (University of Cambridge), Eli Biham (Technion), and Lars Knudsen (University of California San Diego)
- **Twofish**
  - Bruce Schneier, John Kelsey, and Niels Ferguson (Counterpane, Inc.), Doug Whiting (Hi/fn, Inc.), David Wagner (University of California Berkeley), and Chris Hall (Princeton University)

AES


Key
16 Bytes (128 bits)
Expand Key
Plain Text
16 Bytes (128 bits)
Add Round Key
W[0, 3]
Round 1
Substitute Bytes
Shift Rows
Mix Columns
Add Round Key
W[4, 7]
Round 9
Substitute Bytes
Shift Rows
Mix Columns
Add Round Key
W[36, 39]
Round 10
Substitute Bytes
Shift Rows
Add Round Key
W[40, 43]
Cipher Text
16 Bytes (128 bits)

VERSIONS OF AES

- Rijndael supports block sizes and key sizes of 128, 160, 192, 224 and 256 bits.
- Only 128-bit block size, and 128, 192, and 256 key sizes are specified in the AES.

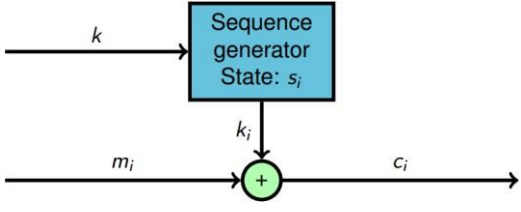
Version	Key Size	Number of rounds
AES-128	128 bits	10
AES-192	192 bits	12
AES-256	256 bits	14

AES KEY SIZE

- Uses really big numbers
  - 1 in 2^{61} odds of winning the lotto and being hit by lightning on the same day
  - 2^{92} atoms in the average human body
  - 2^{128} possible keys in AES-128
  - 2^{170} atoms in the planet
  - 2^{190} atoms in the sun
  - 2^{192} possible keys in AES-192
  - 2^{233} atoms in the galaxy
  - 2^{256} possible keys in AES-256

STREAM CIPHER

- A faster alternative for encryption is a stream cipher.
- We generate a pseudorandom *key stream* from a seed, a "real key" much shorter than the full key stream added to the message.
- We try to make the set of possible seeds, the real keys, so large that exhaustive search is impossible in practice.
- We try to eliminate any shortcuts to finding this key from the key stream.



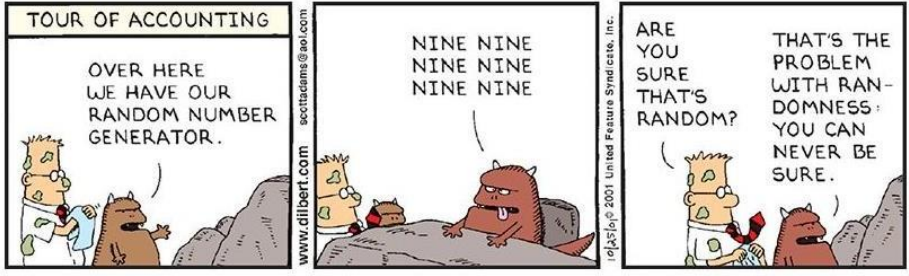
$$s_i = f(k, s_{i-1})$$

$$k_i = g(s_i)$$

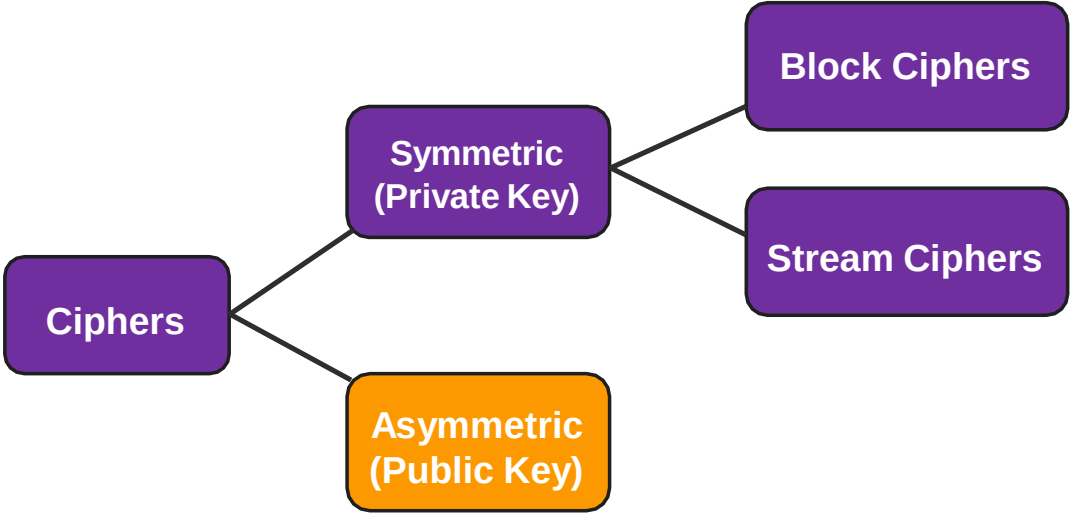
$$c_i = m_i \oplus k_i$$

TESTING RANDOMNESS

- There are RNG tests have been collected into test suites to examine the randomness of a generated bitstream.
  - **Diehard** (Marsaglia, 1995), good for simple PRNGs, but not well-documented
  - **NIST STS** (2010), well documented but from NIST
  - **Dieharder** (Brown et al, 2013), easy to use and well documented
- Can I use randomness tests to make sure my PRNG's output is random?



CLASSIFICATION OF CRYPTOSYSTEMS



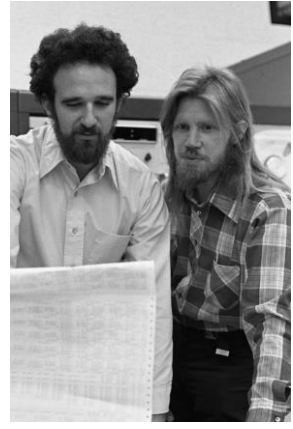
PROBLEMS WITH SYMMETRIC CIPHERS

- **Key management**: changing the secret key or establishing one is nontrivial.
  - Change the keys two users share (should be done reasonably often)
  - Establish a secret key with somebody you do not know and cannot meet in person: (e.g., visiting secure websites such as e-shops)
  - This could be done via a trusted Key Distribution Center (KDC)
  - Can (or should) we really trust the KDC?
  - "What good would it do after all to develop impenetrable cryptosystems, if their users were forced to share their keys with a KDC that could be compromised by either burglary or subpoena?" – Diffie, 1988

- **Digital signatures**: a mathematical scheme for demonstrating the authenticity of digital messages or documents

A BREAKTHROUGH IDEA

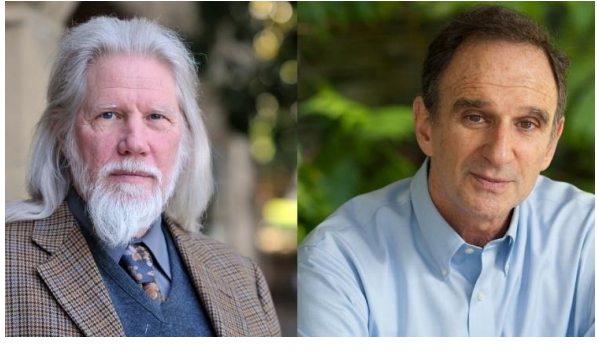
- Rather than having a secret key that the two users must share, each users has **two keys**
- **One key is secret** and he is the only one who knows it
- **The other key is public** and anyone who wishes to send him a message uses that key to encrypt the message
- Diffie and Hellman's groundbreaking 1976 paper, "New Directions in Cryptography," introduced the ideas of public-key cryptography
- NSA claims to have known it since mid-1960s!
- Communications-Electronic Security Group (British counterpart of NSA) documented the idea in a classified report in 1970.



Martin Hellman & Whitfield Diffie

INVENTION OF PUBLIC KEY CRYPTOGRAPHY

- Diffie and Hellman's invention of public-key cryptography and digital signatures revolutionized computer security



They received the 2015 ACM A.M. **Turing Award** for critical contributions to modern cryptography