

CS810 - Advanced Programming in the UNIX Environment

—

Encryption in a Nutshell

Department of Computer Science
Stevens Institute of Technology
Jan Schaumann

`jschauma@cs.stevens.edu`

`http://www.cs.stevens.edu/~jschauma/810-APUE/`

Why use encryption?

- personal privacy
 - “juicy” personal conversations
 - private information that might reveal other information
 - shopping history / personal interests → profile
 - safety from persecution based on “forbidden” activities
- business secrets
 - passwords to other systems
 - salary information
 - other people’s private information
 - insider information

Why use encryption?

- personal privacy
 - “juicy” personal conversations
 - private information that might reveal other information
 - shopping history / personal interests → profile
 - safety from persecution based on “forbidden” activities
- business secrets
 - passwords to other systems
 - salary information
 - other people’s private information
 - insider information

... and of course, just because you’re paranoid doesn’t mean they’re not after you!

Purpose of Encryption

Encryption provides security in the areas of:

- Authenticity
- Accuracy or Integrity
- Secrecy or Confidentiality

Purpose of Encryption

Encryption provides security in the areas of:

- Authenticity
 - *Is the person I'm talking to who I think it is?*
- Accuracy or Integrity
- Secrecy or Confidentiality

Purpose of Encryption

Encryption provides security in the areas of:

- Authenticity
 - *Is the person I'm talking to who I think it is?*
- Accuracy or Integrity
 - *Is the message I received in fact what was sent?*
- Secrecy or Confidentiality

Purpose of Encryption

Encryption provides security in the areas of:

- Authenticity
 - *Is the person I'm talking to who I think it is?*
- Accuracy or Integrity
 - *Is the message I received in fact what was sent?*
- Secrecy or Confidentiality
 - *Did/could anybody else see the message?*

How does encryption work?

Secrecy: Make sure that the data can only be read by those intended.

How does encryption work?

Secrecy: Make sure that the data can only be read by those intended.

- Alice and Bob agree on a way to transform data
- transformed data is sent over insecure channel
- Alice and Bob are able to get data out of the transformation

How does encryption work?

Secrecy: Make sure that the data can only be read by those intended.

- Alice and Bob agree on a way to transform data
- transformed data is sent over insecure channel
- Alice and Bob are able to get data out of the transformation

Different approaches:

- secret key cryptography
- public key cryptography

How does encryption work?

Secrecy: Make sure that the data can only be read by those intended.

- Alice and Bob agree on a way to transform data
- transformed data is sent over insecure channel
- Alice and Bob are able to get data out of the transformation

Different approaches:

- secret key cryptography (example: *DES*)
 - Alice and Bob share a secret
 - Alice can prove to Bob that she knows a secret
- public key cryptography

How does encryption work?

Secrecy: Make sure that the data can only be read by those intended.

- Alice and Bob agree on a way to transform data
- transformed data is sent over insecure channel
- Alice and Bob are able to get data out of the transformation

Different approaches:

- secret key cryptography (example: *DES*)
 - Alice and Bob share a secret
 - Alice can prove to Bob that she knows a secret
- public key cryptography (example: *RSA*)
 - Alice has a private and a public key
 - data encrypted with her private key can only be decrypted by her public key and vice versa
 - public key can be shared with Bob

Accuracy or Integrity

In order to protect against forgery or data manipulation, provide some sort of digest or checksum (often a one-way hash). Popular choices:

- 5f4dcc3b5aa765d61d8327deb882cf99
- 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
- 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

Accuracy or Integrity

In order to protect against forgery or data manipulation, provide some sort of digest or checksum (often a one-way hash). Popular choices:

- 5f4dcc3b5aa765d61d8327deb882cf99 (MD5)
- 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 (SHA-1)
- 5e884898da28047151d0e56f8dc6292773603d0d6aabdd62a11ef721d1542d8 (SHA256)

Accuracy or Integrity

In order to protect against forgery or data manipulation, provide some sort of digest or checksum (often a one-way hash). Popular choices:

- 5f4dcc3b5aa765d61d8327deb882cf99 (MD5)
- 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 (SHA-1)
- 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 (SHA256)

Caveats:

- “rainbow tables” / internet search engines allow for easy reverse lookup of un-salted hashes.
- integrity only ensured if authenticity of information itself is guaranteed

Authenticity

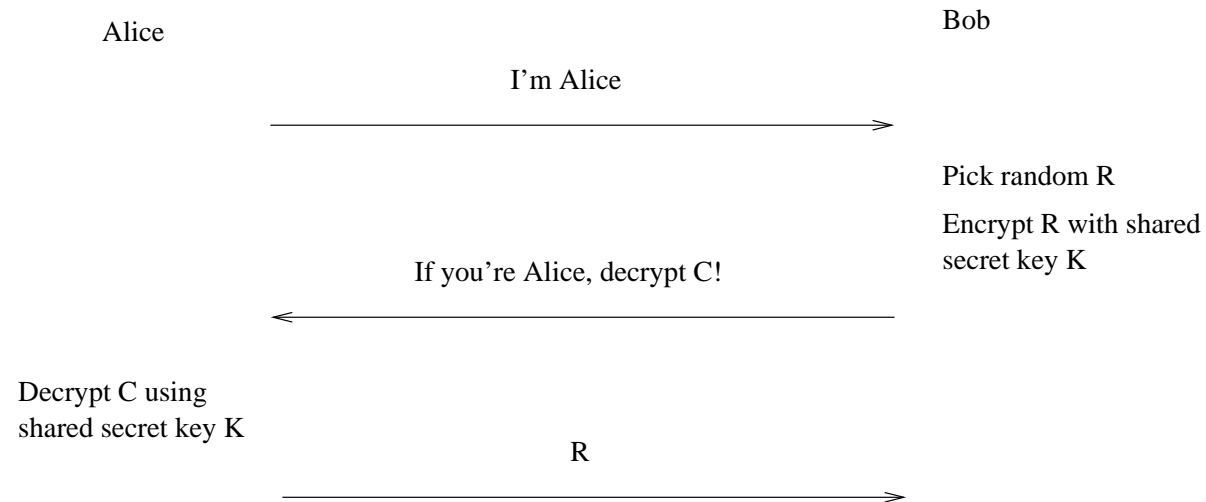


Authenticity

- in private key cryptography, authenticity is (often) assumed/implied
- in public key cryptography, often accomplished via a separate signature
- ways to establish assurance of authenticity for parties that have never met:
 - public key infrastructures (PKI) and certificate authorities (CA)
 - “web of trust”

Authentication

First, the client needs to prove that it knows the secret. This is done in the encryption handshake, consisting of a *challenge* and a *response*.

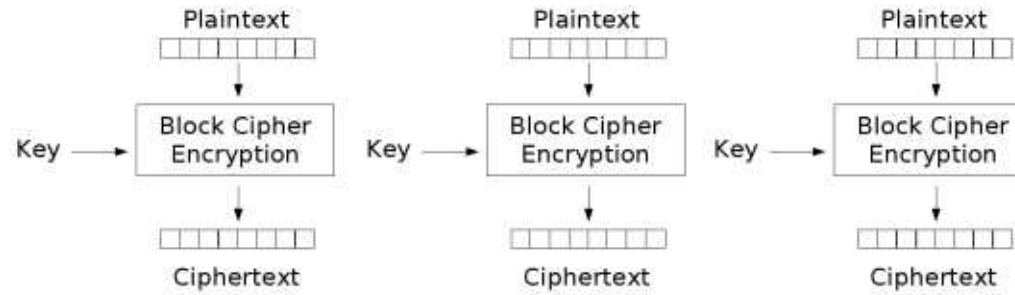


Blowfish

See `openssl_blowfish(3)`:

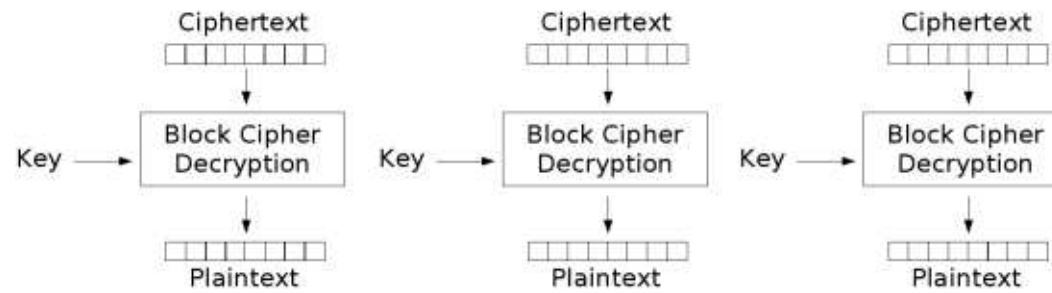
- a symmetric block cipher
- variable key length (we'll use 128 bit)
- consists of a key setup phase and the actual encryption or decryption
- use of `ivec`, which needs to be shared

Cipher Block Chaining: ECB



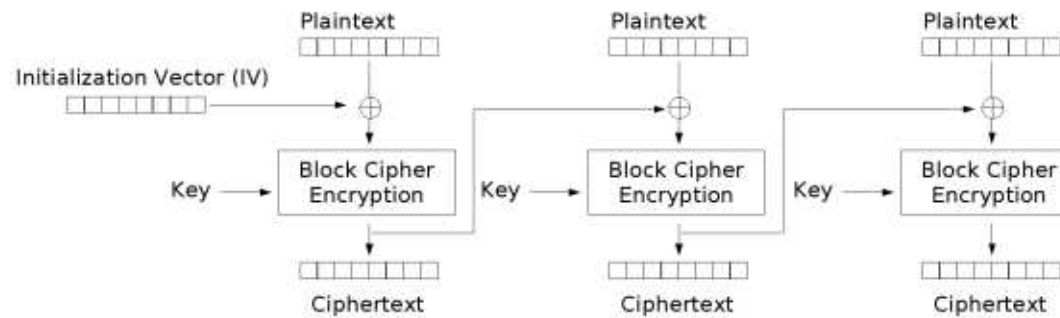
Electronic Codebook (ECB) mode encryption

Cipher Block Chaining: ECB



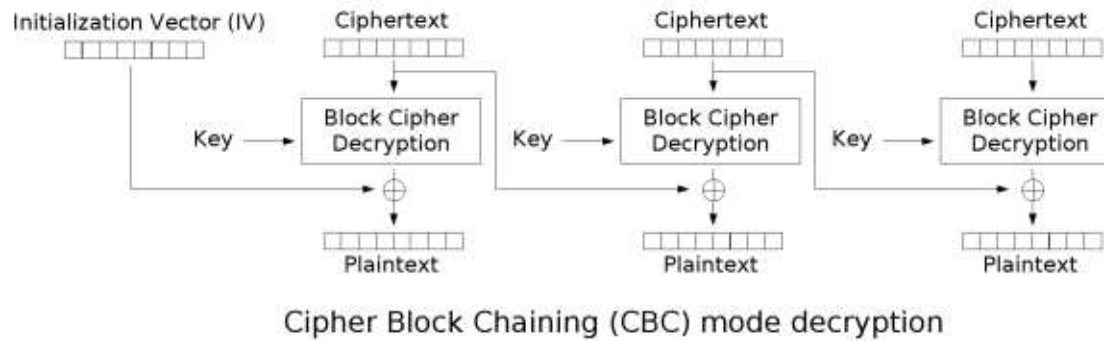
Electronic Codebook (ECB) mode decryption

Cipher Block Chaining: CBC

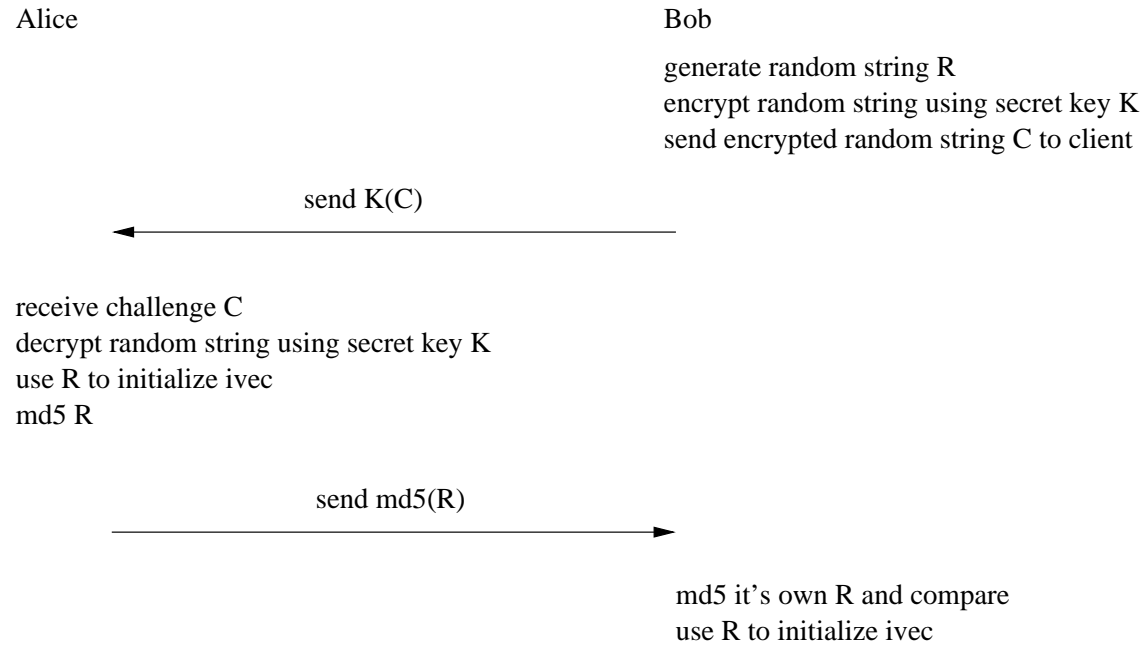


Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining: CBC



Sharing a per-session `ivec`



References

Cryptographic hash functions:

- http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf
- <http://www.gdataonline.com/>

OpenSSL's crypto libraries:

- `EVP_EncryptInit(3)`
- <http://www.linux.org.tw/CLDP/LG/2003/02/vinayak.html>
- http://en.wikipedia.org/wiki/Cipher_Block_Chaining