

在线支付实战

微信支付

讲师: 环环





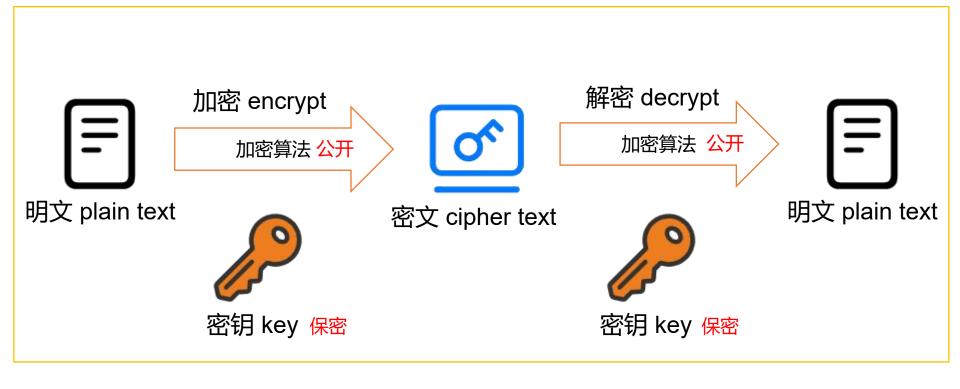
- 1. 微信支付介绍和接入指引
- 2. 证书/秘钥/签名
- 3. 案例项目的创建
 - SpringBoot+Vue
 - Java、MyBatis-Plus、MySQL
 - HTML、JavaScript、Vue
- 4. 基础支付API V3
- 5. 基础支付API V2



- 1. 完整的视频、课件、笔记、源码
- 2. 一套教程从基础理论到应用实践,支付小白轻松入门
- 3. 案例专门针对支付业务开发,包含完整的API接入流程
- 4. 基于流行的SpringBoot+Vue架构,可直接接入常见项目
- 5. 涵盖API V3 和 V2, 满足更多企业应用场景

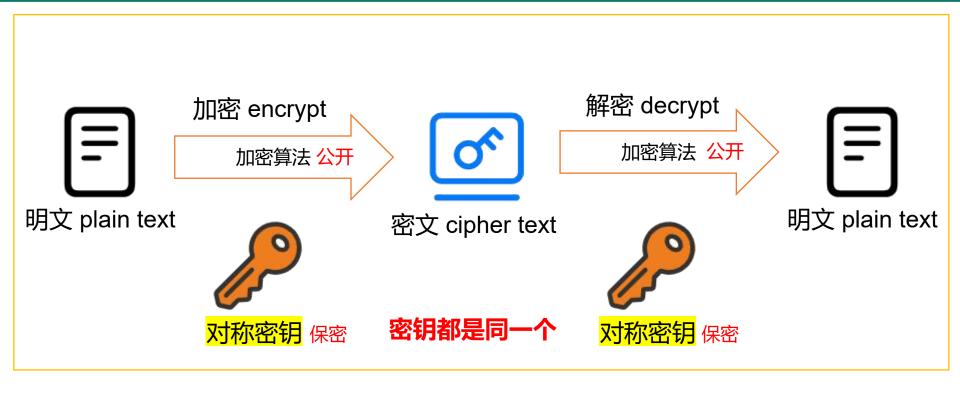






- 密钥的度量单位是位 bit, 如, 秘钥长度128, 就是16字节的二进制串
- 按照密钥的使用方式,加密可以分为两大类:对称加密和非对称加密

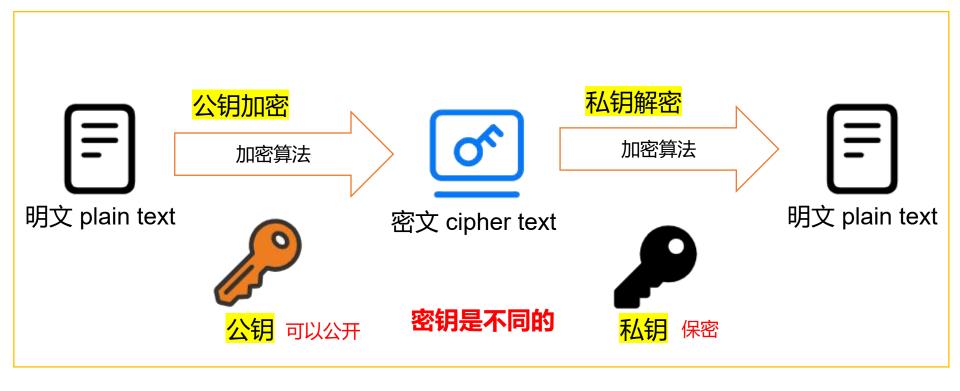




- AES加密算法,密钥长度128、192或256,安全强度很高,性能很好
- 加密分组模式:将明文分组加密,微信支付中使用 AEAD_AES_256_GCM







- 使用公钥加密后只能用私钥解密,反过来,私钥加密后也只能用公钥解密
- RSA加密算法: 最著名的非对称加密算法





对称加密

- 优点:运算速度快
- 缺点: 秘钥需要信息交换的双方共享, 一旦被窃取, 消息会被破解

非对称加密

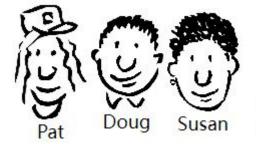
- 优点:私钥严格保密,公钥任意分发,黑客获取公钥无法破解密文
- 缺点:运算速度非常慢

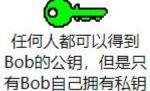


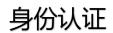
















写信

"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"



HNFmsEm6Un BejhhyCGKOK JUxhiygSBCEiC 0QYIh/Hn3xgiK BcyLK1UcYiY lxx2lCFHDC/A



收信

BejhhyCGKOK
JUxhiygSBCEiC
0QYIh/Hn3xgiK
BcyLK1UcYiY
lxx2lCFHDC/A

yEGDuoj/0F4

MoF8PyYN5Me

HNFmsEm6Un

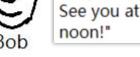


(Bob's private key)

Decrypt with Private Key "Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"



"Hey Susan, See you at







(Susan's public key)



yEGDuoj/0F4 MoF8PyYN5Me jcHXF2NTPzF 0A3+PfqKlQ=



jcHXF2NTPzF 0A3+PfqKlQ= 收信



(Susan's private key)



"Hey Susan, See you at noon!"









yEGDuoj/0F4 MoF8PyYN5Me jcHXF2NTPzF 0A3+PfqKIQ=





yEGDuoj/0F4 MoF8PyYN5Me jcHXF2NTPzF 0A3+PfqKIQ=



(Bob's public key)



"Hey Susan, See you at noon!"









yEGDuoj/0F4 MoF8PyYN5Me jcHXF2NTPzF 0A3+PfqKIQ=



yEGDuoj/0F4 MoF8PyYN5Me jcHXF2NTPzF 0A3+PfqKlQ=



(Bob's public key)



"Hey Susan, See you at noon!"







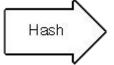
First the created of IGO Overty Good Privary), a published exception of what he had been asset to be protected of electronic mail. State IGO was published constantly as foreward in larve of IGO, if his spread ongoing the first of the transfer that the first hand without the first hand the first hand working asset to the first hand the IGO Charles the IGO Charles hand the IGO Charles had the IGO Charles hand the IGO Charles had been also been supported by the IGO Charles had the IGO Charles had been supported by the IGO Charles had the IGO Charles had been supported by the IGO Charles had been supported b

Comparison were developed in securities; in World West Brook by the based codes. College people of it in these codes. Occapitates because may need now in resultant and too depending. Some people possible of the first wood, if never he code for except the code is not expendent of the first wood, if never he code for except the code for any except distant. Now a code for exception. Some of the presentant of west of the first way and of the code for any exception. Some of the presentant of the exception of the code for the

如何保证信件不被篡改,即信息的完整性?

实现完整性的手段主要是摘要算法 (Digest Algorithm) 也就是常说的散列函数、哈希函数 (Hash Function)

Z



H

"a" => 0cc175b9c0f1b6a831c399e269772661

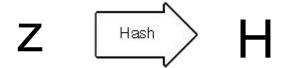
任意长度

固定长度

"aaa" => 47bce5c74f589f4867dbd57e9ca9f808

数据指纹、摘要 (Digest)





任意长度

固定长度

数据指纹、摘要 (Digest)

- 1. 不可逆:只有算法,没有秘钥,只能加密,不能解密
- 2. 难题友好性: 想要破解, 只能暴力枚举
- 3. 发散性: 只要对原文进行一点点改动, 摘要就会发生剧烈变化
- 4. 抗碰撞性:原文不同,计算后的摘要也要不同

常见摘要算法: MD5、SHA1、SHA2 (SHA224、SHA256、SHA384)

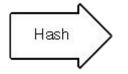






Fin the convex of IGO Orienty Good Privary), a publishery conception activates published to be protection of alternous mail. Since IGO was published deceased in by a few war in how of 1993, the supermed regional tipe if one the world, and has since become the de inthe worldwide reading for every five the time of the monthly control to large large of the major and the surface of the supermedia for the protection of the surface of the surf

Georgestra were developed in securities in World We E modely be local color. College people of in the securities to computers because they were made in number and two expendities. Some people portained that there would never be a reset for more than half is discretized in the security and seem and that not have grouple would name have a need to except their because the presentant of a securities of the security of the securities of the presentant of a securities of the securi



Message Digest



First the contrast of NOP directly Good Privary, a published conception and extrame prolong and the protections of alternature mail. State 1007 was published decounted by an increase in June 41909, it has spread appeal to 1940 over the world and that since become the 6th intermediate of the contrast of the since become the 6th intermediate of the contrast of the since and the contrast of the con

Comparison were developed in securities in World Wire II mainly to break motion. Children's personal of it with here worse to computers between the control of the comparison of the children was the invasion of two deposition. Some people portained that there would never be a need for more than half is discure comparison in the country of a some and their colds any people would nerve in the country of an earn and their colds any people would nerve be a need to be general and any of the comparison. Some of the general cold never the destination through some form of all proveds and invarious the old estimates them not dramps are in Why second contrary people aneath of hower second people of proplets need to have second people of oppositions.





Fin the convex of FGP diverty Good Privary), a philipsing contexpoint activative participate the protections of discretization small. State FGP was published deceased subject increases in large of FGP, it is expended applied they all over the verification that since become the deceased subject in the verification of the state become the deceased of the contraction of the state of the stat

Comparison were developed in securities in Wield West Excisely to beselve order. College people of it on her contests to comparison because they need not in Australia and to organize the production of the three records or expenditure. Some people possible of the three records or records are to comparison in the contest, and a sent and that coding people would not the three a cond for expenditure. Seem of the permittender in the contest of the permittender in the production of the permittender in the production of the permittender in the people of the peopl





比对二者是否一致,如果一致, 信件是就是Bob发的,并且没 有经过篡改

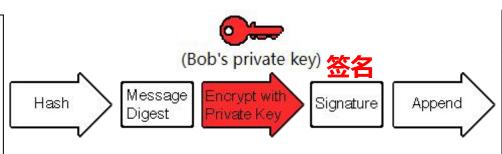






First the cross our of ICO O'verty Good Proving), a published constraint and the protection of allocation and many publicate for the protection of allocation and many financial published documents by a thorward in large of ICO, if the spread organized by all over the weight, and that a time fraction the first hand with a first the first hand when the first hand the first hand the protection of the first product of an analysis of the first product of the first product of the first wave from the first product of the first wave from the first first product of the first wave from the first product of the first wave from the first first product of the first

Comparison were developed in securities in Week! Whe Encickly behaved notice. Collecting people of it in these context. Occapations because may never some in resultance and two depositive. Some people power land that here weeked never be a result for extend that half is done comparison in the context, and some used that notifie any people would name in here a need two comparison. Some of the presentance of two contexts and the context of the presentance of the pres



First the creation of IGO (Freely Good Provincy), a publishing energy-time activation and though the the protection of electronic mail: State IGO was published documentably to the result in himself 1992. It has a greated appellably all over the world, and that a time fracture the of hists worldwide straction for energy-time with annice fracture the of hists worldwide straction for the energy-time with a mail variously annual part ways. For these small rate of the time of the times of the time of the times of times of the times of th

Gouga term were developed in securities in Weeld Wee II mainly be been codes. Children project for it in these content is comparise; because may mean over in relative and two expendities choose people possible of the first revealed are the project for the content data. Intil it does monapation in the country, and seem and that coding project would name that we need to week anything the long were termed in at that years of the content of the project and the content of the project and the project is seen to be a seen of the content of the project and the project is seen to the content of the project and the project is seen to the content of the project is seen to the content of the content

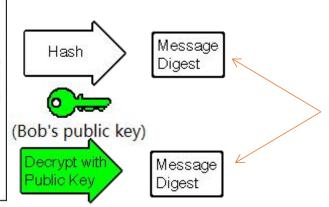
Signature



Fix the criss was of 100° diverty Good Provings, a publishing conception is offering published decounterfluid, and fixed was published decounterfluid; and fixed was published decounterfluid; an increase in large of 1993, I have greated applied they if a root to worth and an increase the first that worldwide is decided the encounterfluid and an increase the contraction of the contraction was of the contraction of the contraction was of the contraction of the contraction of the contraction was often of the contraction of t

George-tran verse developed in recent back in World Was I mainly be based acides. College people of it on her wowers in computers because they need not in number and to opposition possible of her her would never be a received in concern than back dozen computers in the accountry, and seem and that coll any grouph would name in her a received her and the grow-manner of the generation of the previous area of the college of the production of the previous area of the previous area of the previous area of the previous area of the previous and the previous area of the previous area.

Signature



验签

比对二者是否一致,如果一致, 信件是就是Bob 发的,并且没有 经过篡改 Fits the creation of FGP Overly Good Privately a publishing contribute activation and the profession of electronic mail. Stand FGP was published documents by a thereton in these of 1970, if his spread copy half will be received by a thereton in hour of 1970, if his spread copy half will be considered to the other his mail who the contribution of the contribution o

Computer were developed in securities in World West Receivily to best accides. Others propied to it in how consist to computers, because they need not in Anaber and too expendities. Some people possible that them would never be a read for more than half is done more partial in the country, and seem and that not first propied above more partial in the country, and seem and that not first propied without terms of anytogo pith today were formed in that provide and waves the old stimulate into any own of the propied and waves the old stimulate into any own propied propied and the later areas a con-



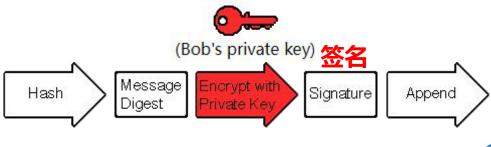






I'm the creates of IOP O'very Good Privary's a publishing energy time activents privary for the proteins of electronia mail: State IOP was published consertingly a free train in June of IVII, if the signed angulated published for the state of the train to be the continue for the last has state of the train the continue for the last has been been been described as a first state of the train and a state of the last privary for the state prival in the last state of the last stat

Comparing were developed in secret back in World War Enterinly to break notice. Ordering people (d) and have some to computer to because may see a secret to expend to compare to because may see as to expend to expend to expend to be a secret than ball it doors compared in the contrary as a secret than ball it doors compared in the contrary as the secret of the general market area to see the compared to the growth and the secret than ball it doors compared to the growth and in the secret the secret the secret the secret than the secret the secret the secret than the s



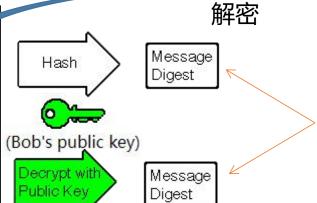
对称加密

Firs the cross of IGO Orety Good Provey), a publishey encomprise activene policy for the preteriors of electronal mail. Since IGO was political foundation by a retermine in law of 1991, it has grown for good thy of over the world and has a non-become the de has a bank of the political form of the political

Signature







验签

比对二者是否一致,如果一致, 信件是就是Bob 发的,并且没有 经过篡改 the previous of FGP directly Good Privated, a published by the notionary parkage for the protection of electronar stati.

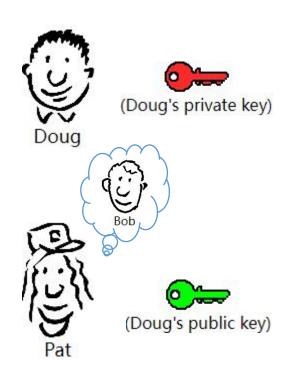
So GGP was published documentably to the revent in hims of 1993, if their general cryptables of the revent is the red of 1993, if their general cryptables of the recognition of the node without the decision for exception of the node without protected when for exception of the node without protected when for their first great or the time for magnetic at contain all an exercipation for the 190 Content decision of the 190 Content decision for t

Gouga tea many developed in receptions in Wheld West Institute the Month of the Continue propied in it in the or season in Companions because may meet now in resultant and the expensive Continue people possible discrete interference would reverbe a receive for except the continue than half-it dense montpotent in the country, and season and their certification management in the country, and season and their certification where a receive for extending are the season of the Continue of the Co









Firs the creator of PGP direty Good Privary), a public key. Firs the cross on of 100° direct (Good Privaria, a published) entropion extreme parties for the protection of indicate at mail. Since 100° was published discountingly a thorours in Jame of 1907, the contract of the published discountingly as the county of the 1907, the of halos methods indicated for every first of the mail variously assuments including a more than 100° or copyling of the mail variously contracts in the published of the copyling of the mail variously recognition, and in one expectation by the 100° current derivate, who are used that here were tooked when 100° purious counted the US. That is weekplaces were closed without indicates in it, is assume 1909.

Comparison were developed in second back in World War II socially be break notice. Ordinary people (b) not have sooned to comparison population of the control to compare the control population of the theory would revers be a rose for more than ball is discorrectly as the form would reverse the control to control the control property for the con people need to have some to good cryptography?



The the creater of RGP directly Good Provent, a public key econyption actives a public for the protection of electronic small. Since RGP was published documents by an increase in June of 1993, Since the "was pursuant accounting on necessary in our of 1997, the signed organical field over the world, and has since become the de inthe medicarda standard for energy-time of 3 mail, making management includes a week standard for energy-time of 3 mail, making management includes a week produced by the 1997 and the produced to regulate a management energy-time of the Course of Section, who assumed that have were broken, when 1907 appear of which the US. That is verification was closed without indictant in faculty 1999.

Comparison were developed in secret back in World Wire Enteinly to benefit solders. Ordinary people (d) and have solders whose to compute the secret solders. Ordinary people of the district solders whose the comparison of the final world in review to a reset for solders than half is shown comparison in the country, and seem and their notifies are people would never have a more for comparison. Seem of the permission of entering the control of the permission of contrary or solders when the control or of the permission of contrary and control or of the comparison of contrary or the control or of the comparison of contrary or the control or of the control or of the contrary to the control or of the control or of the contract or of the contract or of the control people need to have seems to good cryptography?

公钥的信任: 黑客可以伪造公钥, 怎么判断公钥是真实的?





数字证书信息

公钥:

所有者:

颁发者:

.....

• 公钥: Bob的公钥

• 所有者: Bob

• 颁发者: CA (Certificate Authority, 证书认证机构)

• 有效期:证书的使用期限

• 签名哈希算法: 指定摘要算法, 用来计算证书的摘要

• 指纹:证书的摘要,保证证书的完整性

• 签名算法:用于生成签名,确保证书是由CA签发

• 序列号:证书的唯一标识





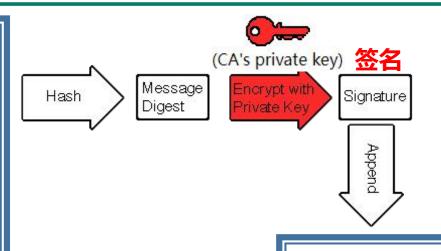
数字证书信息

公钥:

所有者:

颁发者:

.....





数字证书信息

公钥:

所有者:

颁发者:

Signature





First the circular of IGP directly Good Provings is published encouraged and the probabilities of electronic matter. Since FGP was published connectionly as because in June 1978, it has a providing published to exactly as the world one income the de to take more became the de take more became a managed as a man to all as managed on the ICP append on the take who the more of a man to all as managed on the ICP append on the data force were tracked without ICP append on the data the world of the ICP append on the data the world of the ICP append on the data the world of the ICP append on the ICP append

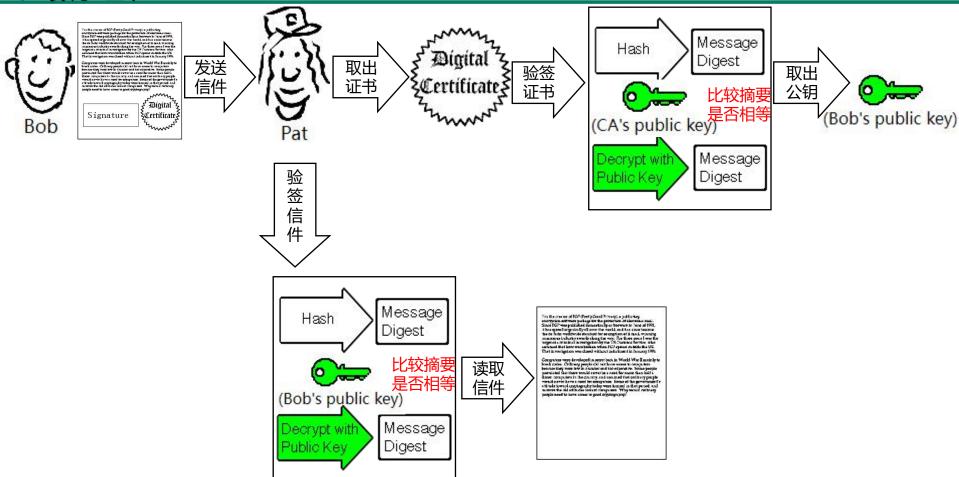
Consyntess were developed in secret back in World Was I mainly to break codes. Ordinary people GM and have some to computers because they seem to a number and too expendition. Some people postulated that their smould networks a resed for more than half a drawn computers in the country, and seem and that technique people would never have a need for exceptions. Some of the personnent's efficient toward anything people which the research applications to the person and an account of the person and the person of the person and account or old attention toward computers. They would contrary people would be have account a good cryptography.

Signature



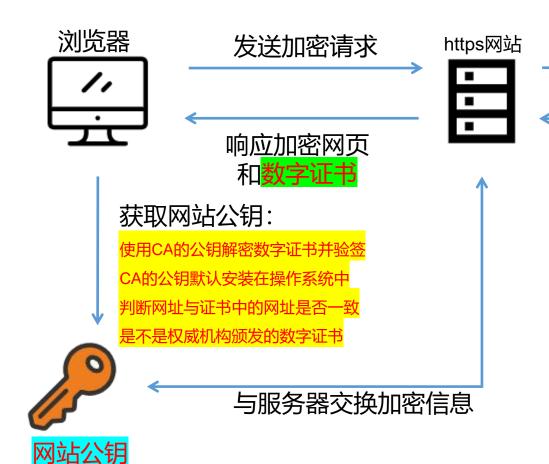












申请数字证书

_____ **CA** 颁发<mark>数字证书</mark>:

CA用私钥加密数字证书并签名

数字证书中存有<mark>网站的公钥</mark>





步骤:

- 1. 创建SpringBoot项目 (Java、SpringBoot、SpringMVC、RESTful、json)
- 2. 引入Swagger (接口文档和测试页面生成工具)
- 1. 定义统一结果(让前后端数据通信更规范)
- 3. 创建和连接数据库 (MySQL、IDEA内置的数据库管理工具)
- 4. 集成MyBatis-Plus (MyBatis)
- 5. 搭建前端环境(了解HTML和CSS、熟悉JavaScript、了解Vue)
- 6. 认识 Vue.js





内容:

- 1. 引入支付参数
- 2. 加载商户私钥
- 3. 获取平台证书和验签器
- 4. 获取HttpClient对象
- 5. API字典和接口规则
- 6. 内网穿透
- 7. API v3





内容:

- 1. 整合APIv2
- 2. APIv2和APIv3的区别
- 3. Native下单
- 4. 支付结果通知



谢谢观看

