



# 在线支付实战

## 微信支付

讲师：环环

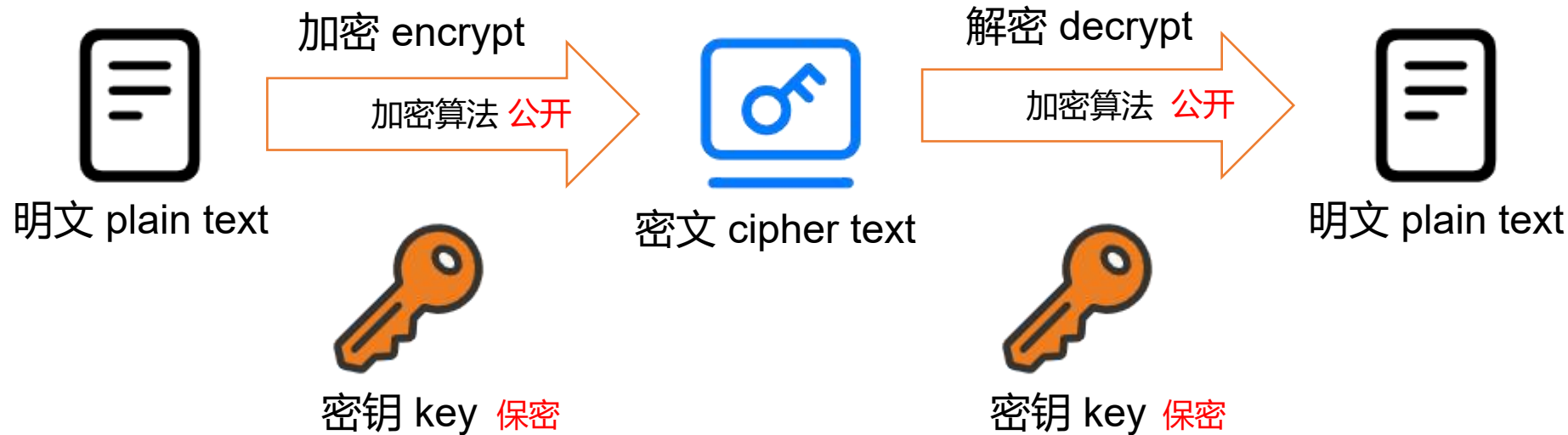
# 目录



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



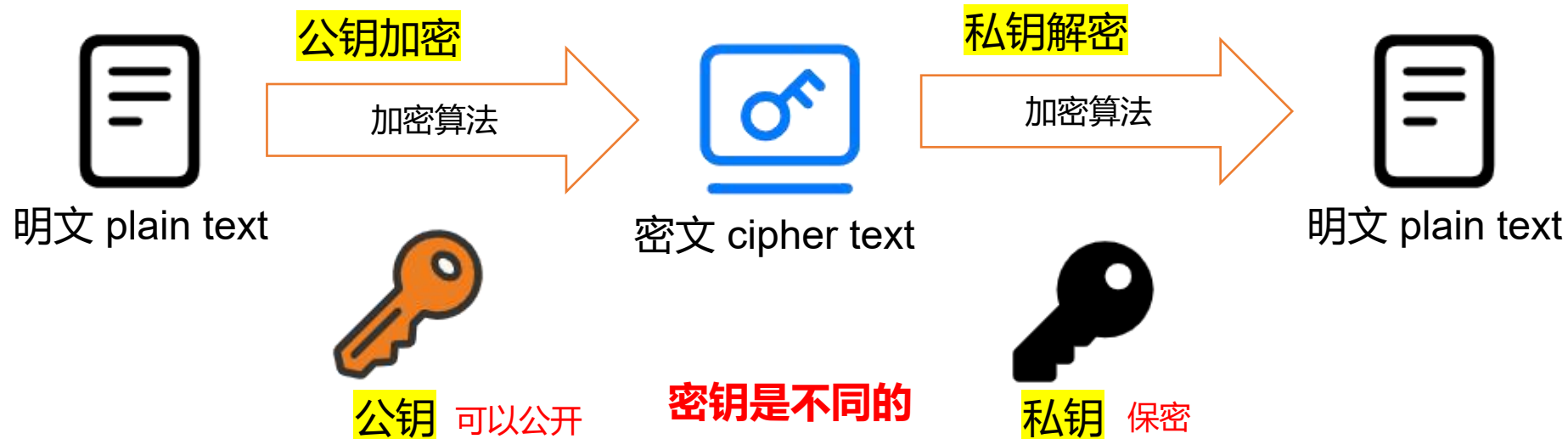
1. 完整的视频、课件、笔记、源码
2. 一套教程从基础理论到应用实践，支付小白轻松入门
3. 案例专门针对支付业务开发，包含完整的API接入流程
4. 基于流行的SpringBoot+Vue架构，可直接接入常见项目
5. 涵盖API V3 和 V2，满足更多企业应用场景



- **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：密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



Bob



(Bob's public key)



(Bob's private key)



Pat



Doug

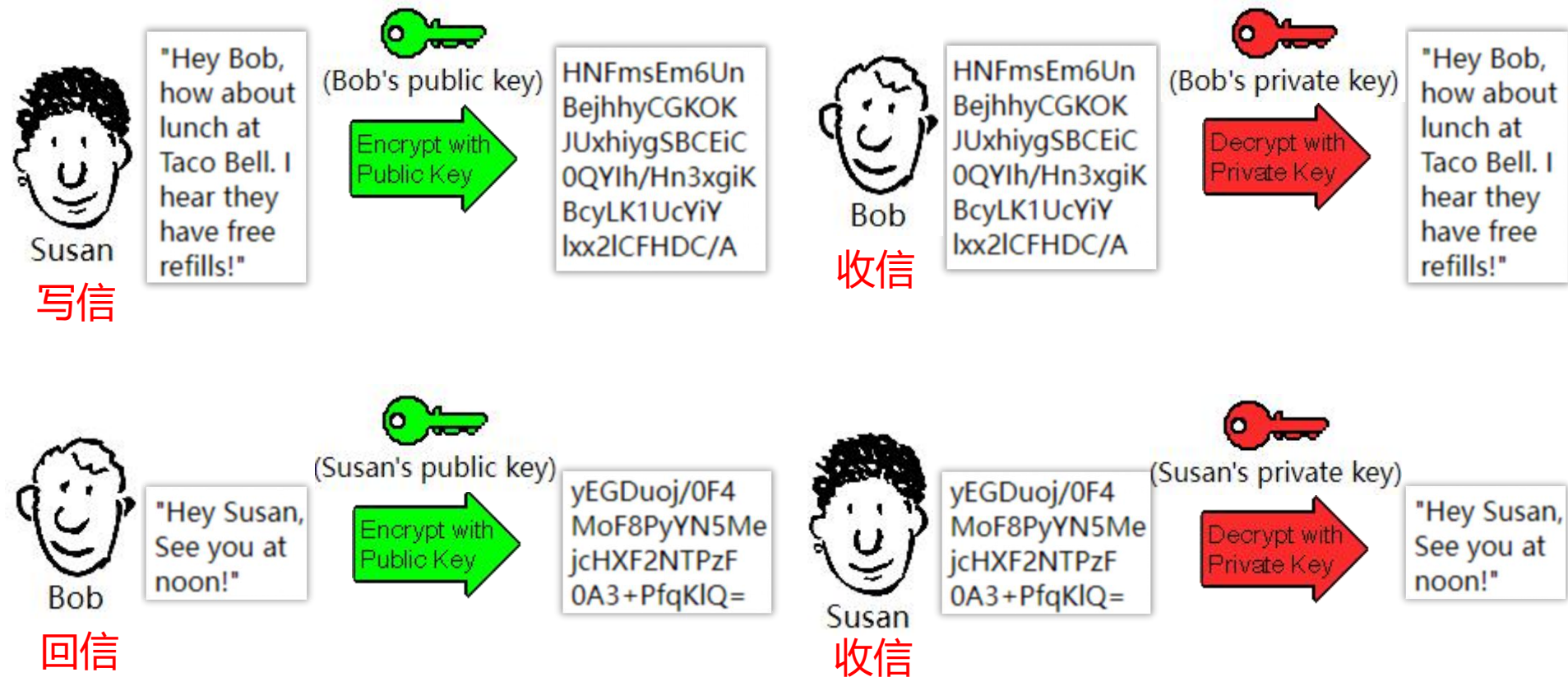


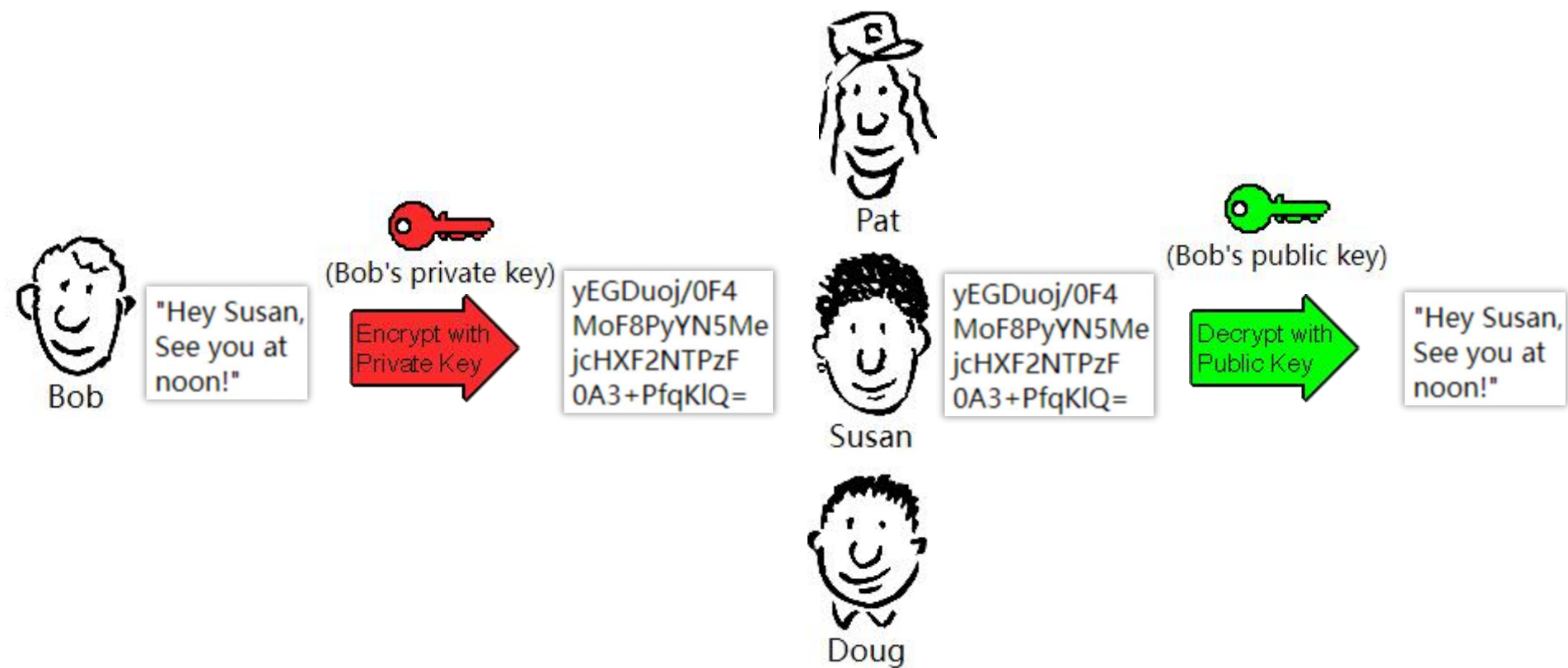
Susan

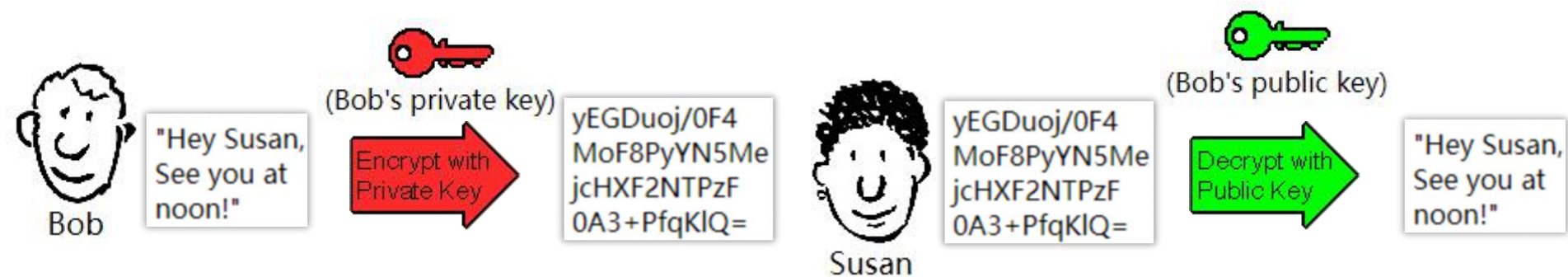


任何人都可以得到  
Bob的公钥，但是只  
有Bob自己拥有私钥







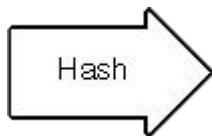




如何保证信件不被篡改，即信息的完整性？

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）



1. 不可逆：只有算法，没有密钥，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)



# 摘要算法和数据的完整性



Bob

This is the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1995, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of e-mail, winning numerous industry awards along the way. For three years I was the target of a relentless investigation by the US Customs Service, who suspected that letters were broken when PGP passed outside the US. That investigation was closed without incident in January 1999.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too in number and too expensive. Some people panicked that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for encryption. Some of the government's attitude toward cryptography today were formed in that period, and to some the old attitudes toward computers. Why would ordinary people need to have access to good encryption?

Hash

Message  
Digest

Append

Message  
Digest

This is the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1995, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of e-mail, winning numerous industry awards along the way. For three years I was the target of a relentless investigation by the US Customs Service, who suspected that letters were broken when PGP passed outside the US. That investigation was closed without incident in January 1999.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too in number and too expensive. Some people panicked that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for encryption. Some of the government's attitude toward cryptography today were formed in that period, and to some the old attitudes toward computers. Why would ordinary people need to have access to good encryption?

Hash

Message  
Digest

Message  
Digest



Pat

This is the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1995, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of e-mail, winning numerous industry awards along the way. For three years I was the target of a relentless investigation by the US Customs Service, who suspected that letters were broken when PGP passed outside the US. That investigation was closed without incident in January 1999.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too in number and too expensive. Some people panicked that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for encryption. Some of the government's attitude toward cryptography today were formed in that period, and to some the old attitudes toward computers. Why would ordinary people need to have access to good encryption?

比对二者是否一致，如果一致，信件就是Bob发的，并且没有经过篡改





Bob

It's the creator of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, security has become a focus of 1995, it has spread rapidly all over the world, and has since become the de facto worldwide standard for encryption of e-mail, making numerous industry events along the way. For three years I was the target of a criminal investigation by the US Customs Service, who suspected that letters were broken when PGP opened outside the US. That investigation was closed without incident in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too big, too slow and too expensive. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and to some extent still influence how it operates. Why would ordinary people need to have access to good cryptography?



Pat

It's the creator of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, security has become a focus of 1995, it has spread rapidly all over the world, and has since become the de facto worldwide standard for encryption of e-mail, making numerous industry events along the way. For three years I was the target of a criminal investigation by the US Customs Service, who suspected that letters were broken when PGP opened outside the US. That investigation was closed without incident in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too big, too slow and too expensive. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and to some extent still influence how it operates. Why would ordinary people need to have access to good cryptography?

Signature



(Bob's private key) **签名**



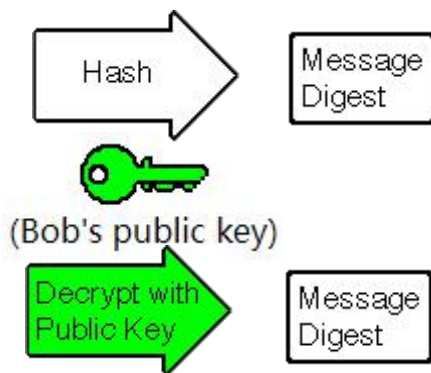
Signature

It's the creator of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, security has become a focus of 1995, it has spread rapidly all over the world, and has since become the de facto worldwide standard for encryption of e-mail, making numerous industry events along the way. For three years I was the target of a criminal investigation by the US Customs Service, who suspected that letters were broken when PGP opened outside the US. That investigation was closed without incident in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too big, too slow and too expensive. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and to some extent still influence how it operates. Why would ordinary people need to have access to good cryptography?

**验签**

比对二者是否一致，如果一致，信件就是Bob发的，并且没有经过篡改



(Bob's public key)

It's the creator of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, security has become a focus of 1995, it has spread rapidly all over the world, and has since become the de facto worldwide standard for encryption of e-mail, making numerous industry events along the way. For three years I was the target of a criminal investigation by the US Customs Service, who suspected that letters were broken when PGP opened outside the US. That investigation was closed without incident in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too big, too slow and too expensive. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and to some extent still influence how it operates. Why would ordinary people need to have access to good cryptography?



# 数字签名 + 对称加密消息原文



Bob

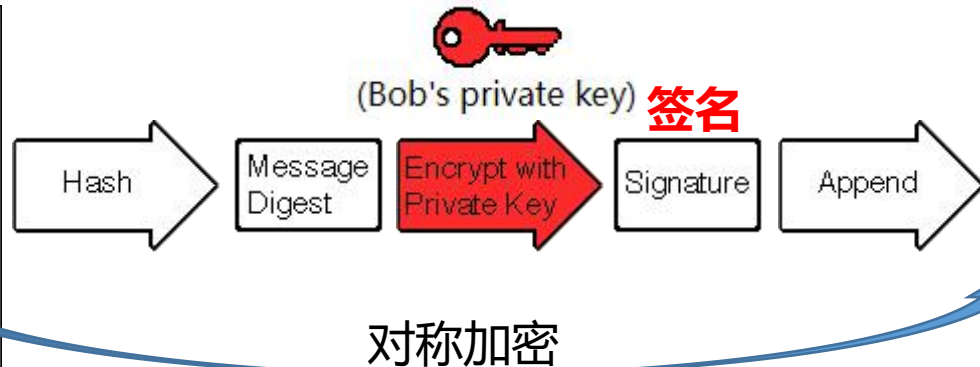
Try the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, electronically signed messages in June of 1991, it has spread rapidly all over the world, and has since become the de facto worldwide standard for encryption of e-mail, making anonymous industry events along the way. For three years I was the target of a criminal investigation by the US Customs Service, who suspected that I was involved in the export of goods to the US. That investigation was closed without incident in January 1995.

Cryptopunks were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too expensive and too expensive. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and to reverse the old attitude toward computers. Why would ordinary people need to have access to good cryptography?

Try the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, electronically signed messages in June of 1991, it has spread rapidly all over the world, and has since become the de facto worldwide standard for encryption of e-mail, making anonymous industry events along the way. For three years I was the target of a criminal investigation by the US Customs Service, who suspected that I was involved in the export of goods to the US. That investigation was closed without incident in January 1995.

Cryptopunks were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too expensive and too expensive. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and to reverse the old attitude toward computers. Why would ordinary people need to have access to good cryptography?

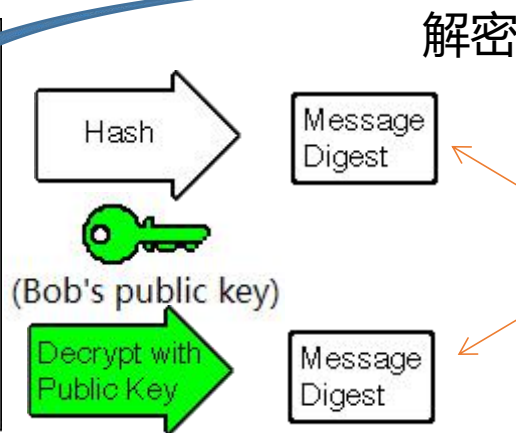
Signature



对称加密



Pat



验签

比对二者是否一致，如果一致，信件就是Bob发的，并且没有经过篡改

Try the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, electronically signed messages in June of 1991, it has spread rapidly all over the world, and has since become the de facto worldwide standard for encryption of e-mail, making anonymous industry events along the way. For three years I was the target of a criminal investigation by the US Customs Service, who suspected that I was involved in the export of goods to the US. That investigation was closed without incident in January 1995.

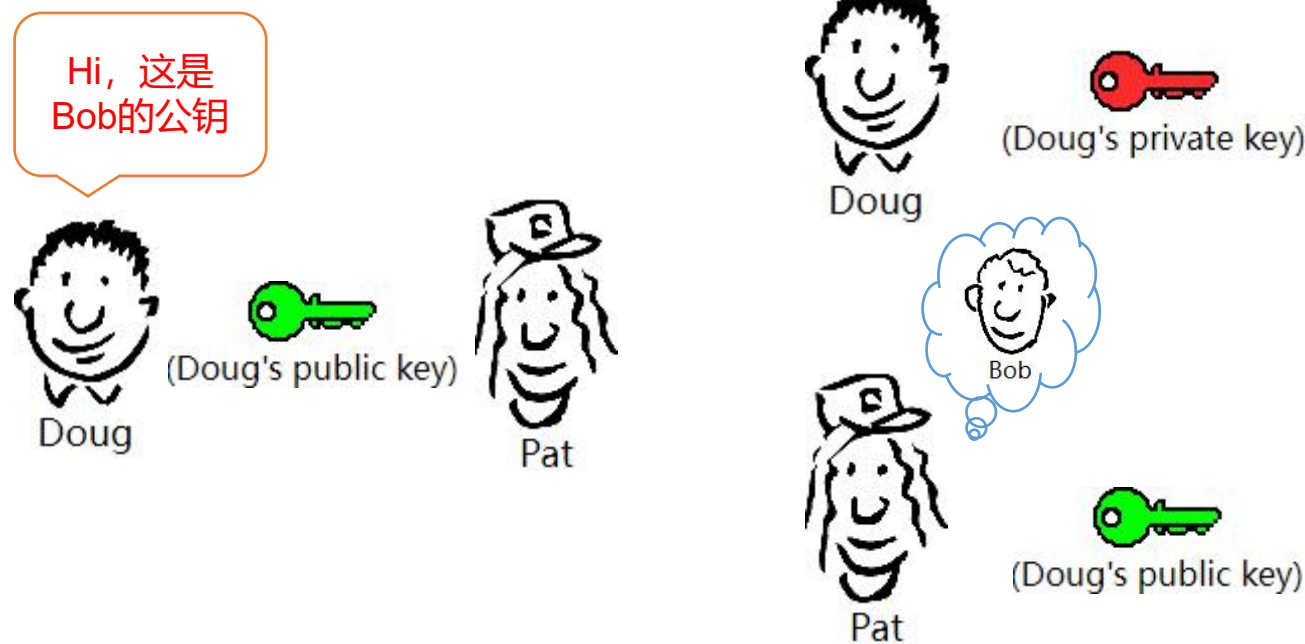
Cryptopunks were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too expensive and too expensive. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and to reverse the old attitude toward computers. Why would ordinary people need to have access to good cryptography?

Signature

Try the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, electronically signed messages in June of 1991, it has spread rapidly all over the world, and has since become the de facto worldwide standard for encryption of e-mail, making anonymous industry events along the way. For three years I was the target of a criminal investigation by the US Customs Service, who suspected that I was involved in the export of goods to the US. That investigation was closed without incident in January 1995.

Cryptopunks were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were too expensive and too expensive. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and to reverse the old attitude toward computers. Why would ordinary people need to have access to good cryptography?





Try the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published documentally as freeware in June of 1991, it has spread organically all over the world, and has since become the de facto mechanism to protect the encryption of e-mail, winning numerous industry awards along the way. But there goes I was the target of a criminal investigation by the FBI Customs Service, who suspected that here were broken when PGP spread outside the US. That investigation was closed without indictment in January 1995.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were not in the hands of the government. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the governments of the world looked at cryptography today were learned in that period, and never the old attitudes toward computers. Why would ordinary people need to have access to good cryptography?

Signature

Try the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published documentally as freeware in June of 1991, it has spread organically all over the world, and has since become the de facto mechanism to protect the encryption of e-mail, winning numerous industry awards along the way. But there goes I was the target of a criminal investigation by the FBI Customs Service, who suspected that here were broken when PGP spread outside the US. That investigation was closed without indictment in January 1995.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were not in the hands of the government. Some people pointed out that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the governments of the world looked at cryptography today were learned in that period, and never the old attitudes toward computers. Why would ordinary people need to have access 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



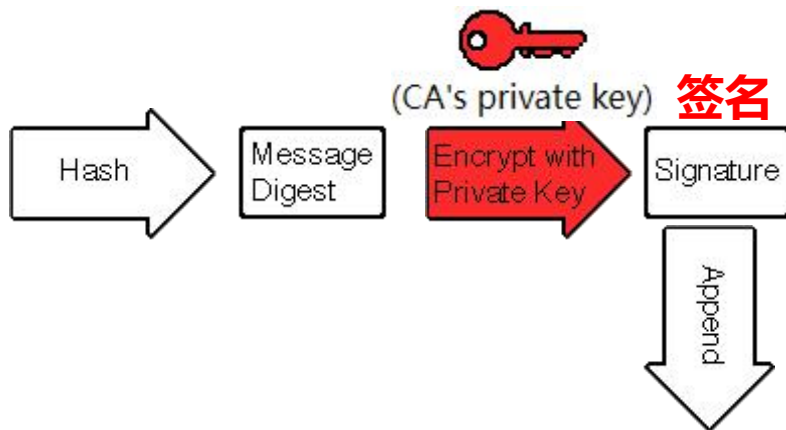
## 数字证书信息

公钥: .....

所有者: .....

颁发者: .....

.....  
.....



## 数字证书信息

公钥: .....

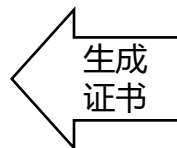
所有者: .....

颁发者: .....

.....  
.....  
Signature



数字证书





Bob

Try the creation of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published commercially as freeware in June of 1991, it has spread cryptically all over the world, and has since become the de facto worldwide standard for encryption of e-mail, winning numerous industry awards along the way. For three years I was the target of a critical investigation by the US Customs Service, who surmised that letters were broken when PGP opened outside the US. That investigation was closed without indictment in January 1995.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were few in number and too expensive. Some people predicted that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for encryption. Some of the predominant attitudes toward cryptography today were formed in that period, and to some the old attitudes toward computers. Why would ordinary people need to have access to good cryptography?

Signature



发送  
信件



Pat

[illegible]

发送信件



Pat

取出  
证书

# Digital Certificate

## 验签证书

Hash

Message  
Digest



## 比较摘要 是否相等

(CA's public key)

Decrypt with  
Public Key

Message  
Digest

取出  
公钥



✓ (Bob's public key)

## 验签信件

Hash

Message  
Digest



## 比较摘要 是否相等

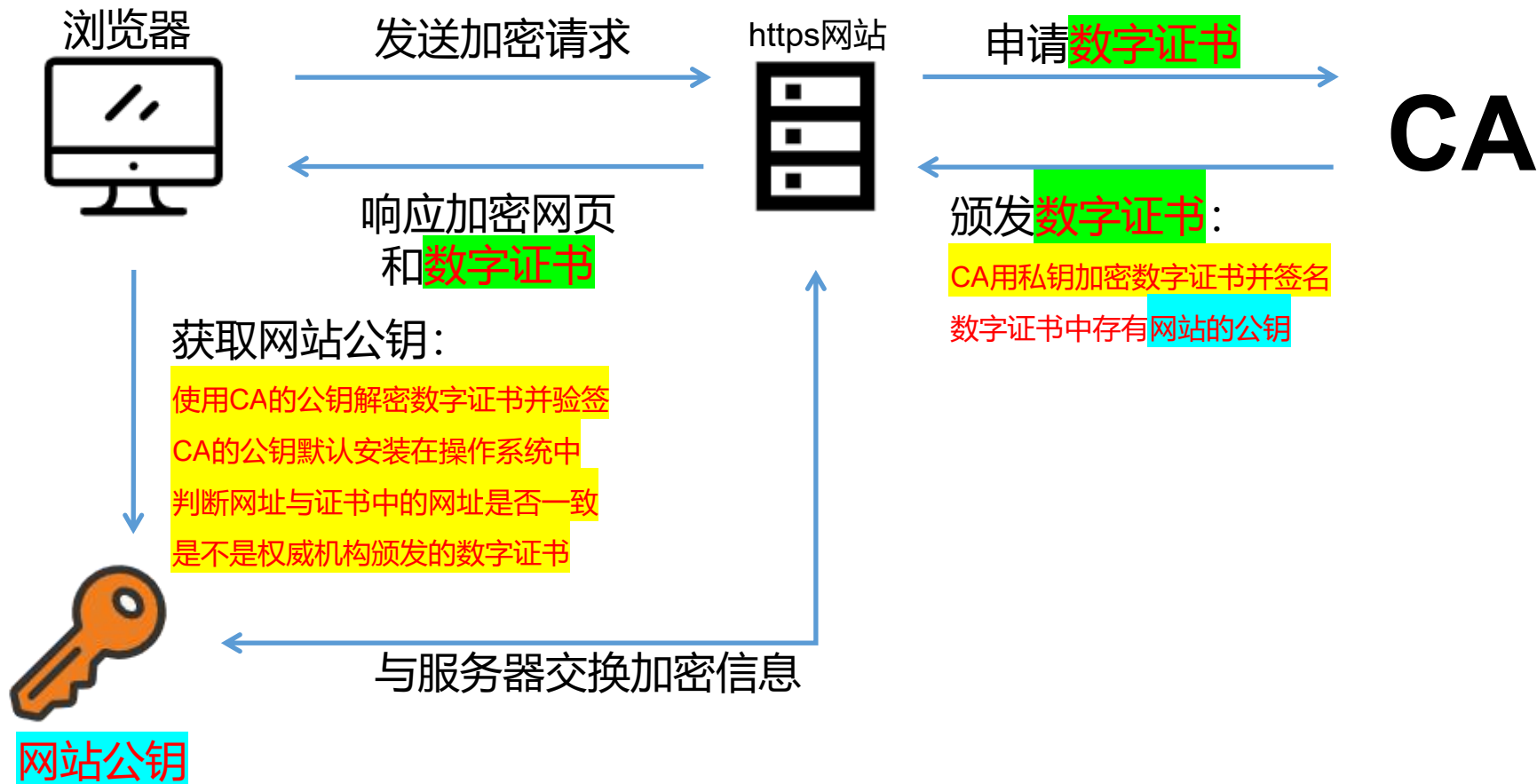
(Bob's public key)

Decrypt with Public Key

Message  
Digest

读取信件

This is the story of *Energy Good Through*, a public energy awareness package for the protection of electronic mail. Since 1976 was published, *Energy Good Through* has been in use in 1978, 1980, 1982, 1984, 1986, 1988, 1990, 1992, 1994, 1996, 1998, 2000, 2002, 2004, 2006, 2008, 2010, 2012, 2014, 2016, 2018, 2020, 2022, 2024, 2026, 2028, 2030, 2032, 2034, 2036, 2038, 2040, 2042, 2044, 2046, 2048, 2050, 2052, 2054, 2056, 2058, 2060, 2062, 2064, 2066, 2068, 2070, 2072, 2074, 2076, 2078, 2080, 2082, 2084, 2086, 2088, 2090, 2092, 2094, 2096, 2098, 2100, 2102, 2104, 2106, 2108, 2110, 2112, 2114, 2116, 2118, 2120, 2122, 2124, 2126, 2128, 2130, 2132, 2134, 2136, 2138, 2140, 2142, 2144, 2146, 2148, 2150, 2152, 2154, 2156, 2158, 2160, 2162, 2164, 2166, 2168, 2170, 2172, 2174, 2176, 2178, 2180, 2182, 2184, 2186, 2188, 2190, 2192, 2194, 2196, 2198, 2200, 2202, 2204, 2206, 2208, 2210, 2212, 2214, 2216, 2218, 2220, 2222, 2224, 2226, 2228, 2230, 2232, 2234, 2236, 2238, 2240, 2242, 2244, 2246, 2248, 2250, 2252, 2254, 2256, 2258, 2260, 2262, 2264, 2266, 2268, 2270, 2272, 2274, 2276, 2278, 2280, 2282, 2284, 2286, 2288, 2290, 2292, 2294, 2296, 2298, 2300, 2302, 2304, 2306, 2308, 2310, 2312, 2314, 2316, 2318, 2320, 2322, 2324, 2326, 2328, 2330, 2332, 2334, 2336, 2338, 2340, 2342, 2344, 2346, 2348, 2350, 2352, 2354, 2356, 2358, 2360, 2362, 2364, 2366, 2368, 2370, 2372, 2374, 2376, 2378, 2380, 2382, 2384, 2386, 2388, 2390, 2392, 2394, 2396, 2398, 2400, 2402, 2404, 2406, 2408, 2410, 2412, 2414, 2416, 2418, 2420, 2422, 2424, 2426, 2428, 2430, 2432, 2434, 2436, 2438, 2440, 2442, 2444, 2446, 2448, 2450, 2452, 2454, 2456, 2458, 2460, 2462, 2464, 2466, 2468, 2470, 2472, 2474, 2476, 2478, 2480, 2482, 2484, 2486, 2488, 2490, 2492, 2494, 2496, 2498, 2500, 2502, 2504, 2506, 2508, 2510, 2512, 2514, 2516, 2518, 2520, 2522, 2524, 2526, 2528, 2530, 2532, 2534, 2536, 2538, 2540, 2542, 2544, 2546, 2548, 2550, 2552, 2554, 2556, 2558, 2560, 2562, 2564, 2566, 2568, 2570, 2572, 2574, 2576, 2578, 2580, 2582, 2584, 2586, 2588, 2590, 2592, 2594, 2596, 2598, 2600, 2602, 2604, 2606, 2608, 2610, 2612, 2614, 2616, 2618, 2620, 2622, 2624, 2626, 2628, 2630, 2632, 2634, 2636, 2638, 2640, 2642, 2644, 2646, 2648, 2650, 2652, 2654, 2656, 2658, 2660, 2662, 2664, 2666, 2668, 2670, 2672, 2674, 2676, 2678, 2680, 2682, 2684, 2686, 2688, 2690, 2692, 2694, 2696, 2698, 2700, 2702, 2704, 2706, 2708, 2710, 2712, 2714, 2716, 2718, 2720, 2722, 2724, 2726, 2728, 2730, 2732, 2734, 2736, 2738, 2740, 2742, 2744, 2746, 2748, 2750, 2752, 2754, 2756, 2758, 2760, 2762, 2764, 2766, 2768, 2770, 2772, 2774, 2776, 2778, 2780, 2782, 2784, 2786, 2788, 2790, 2792, 2794, 2796, 2798, 2800, 2802, 2804, 2806, 2808, 2810, 2812, 2814, 2816, 2818, 2820, 2822, 2824, 2826, 2828, 2830, 2832, 2834, 2836, 2838, 2840, 2842, 2844, 2846, 2848, 2850, 2852, 2854, 2856, 2858, 2860, 2862, 2864, 2866, 2868, 2870, 2872, 2874, 2876, 2878, 2880, 2882, 2884, 2886, 2888, 2890, 2892, 2894, 2896, 2898, 2900, 2902, 2904, 2906, 2908, 2910, 2912, 2914, 2916, 2918, 2920, 2922, 2924, 2926, 2928, 2930, 2932, 2934, 2936, 2938, 2940, 2942, 2944, 2946, 2948, 2950, 2952, 2954, 2956, 2958, 2960, 2962, 2964, 2966, 2968, 2970, 2972, 2974, 2976, 2978, 2980, 2982, 2984, 2986, 2988, 2990, 2992, 2994, 2996, 2998, 3000, 3002, 3004, 3006, 3008, 3010, 3012, 3014, 3016, 3018, 3020, 3022, 3024, 3026, 3028, 3030, 3032, 3034, 3036, 3038, 3040, 3042, 3044, 3046, 3048, 3050, 3052, 3054, 3056, 3058, 3060, 3062, 3064, 3066, 3068, 3070, 3072, 3074, 3076, 3078, 3080, 3082, 3084, 3086, 3088, 3090, 3092, 3094, 3096, 3098, 3100, 3102, 3104, 3106, 3108, 3110, 3112, 3114, 3116, 3118, 3120, 3122, 3124, 3126, 3128, 3130, 3132, 3134, 3136, 3138, 3140, 3142, 3144, 3146, 3148, 3150, 3152, 3154, 3156, 3158, 3160, 3162, 3164, 3166, 3168, 3170, 3172, 3174, 3176, 3178, 3180, 3182, 3184, 3186, 3188, 3190, 3192, 3194, 3196, 3198, 3200, 3202, 3204, 3206, 3208, 3210, 3212, 3214, 3216, 3218, 3220, 3222, 3224, 3226, 3228, 3230, 3232, 3234, 3236, 3238, 3240, 3242, 3244, 3246, 3248, 3250, 3252, 3254, 3256, 3258, 3260, 3262, 3264, 3266, 3268, 3270, 3272, 3274, 3276, 3278, 3280, 3282, 3284, 3286, 3288, 3290, 3292, 3294, 3296, 3298, 3300, 3302, 3304, 3306, 3308, 3310, 3312, 3314, 3316, 3318, 3320, 3322, 3324, 3





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