Slide 1: Welcome. Today we will discuss cryptography. Let’s consider two problems. In the first problem, you have a lot of data.

歡迎(大家). 今天, 我們會討論密碼學. 我們來**考慮kǎolǜ**兩個問題. 第一個: 你有很多**數據**.

Huānyíng (dàjiā). Jīntiān, wǒmen huì tǎolùn mìmǎ xué. Wǒmen lái **kǎolǜ** liǎng gè wèntí. Dì yī gè: Nǐ yǒu hěnduō **shùjù.**

Slide 2: Here is an example: you study biology and medicine and have a LOT of DNA data

**1**這是一個例子(or 比如說 bi ru shuo): 你學習生物wù和醫學，並bìng有好多好多的ＤＮＡ數據．

**1**Zhè shì yīgè lìzi: Nǐ xuéxí shēngwù hé yīxué, bìng yǒu hǎoduō hǎoduō de DNA shùjù.

Almost everyone gives you their DNA data. You want to do some important calculations. You could save lives!

差不多，每個人類lèi給妳他們的ＤＮＡ數據．你想要做一些**重**zhòng要的計算.**2**你可以**挽救wǎnjiù**生**命mìng**．

Chàbùduō, měi gèrénlèi gěi nǎi tāmen de DNA shùjù. Nǐ xiǎng yào zuò (yīxiē) **zhòng**yào de jìsuàn.**2** Nǐ kěyǐ **wǎnjiù** shēng**mìng**.

However, it is too much work for you to do yourself!　You need others to help, but can you trust them?

但是，這個計算**量liàng**太大了（有太多數據,**3** 你的電腦太慢了）:你不能自己做了．**4**你還要別的人幫忙，但是你能**相信xiāngxìn**他們呢？

Dànshì, zhège jìsuàn liàng tài dàle (yǒu tài duō shùjù, **3** nǐ de diànnǎo tài mànle): Nǐ bùnéng zìjǐ zuòle.**4** Nǐ hái yào bié de rén bāngmáng, dànshì nǐ néng **xiāngxìn** tāmen ne?

Is it ethical to send the data?

**5發送Fāsòng**數據是不是**合乎héhū**道德？

**Fāsòng** shùjùshìbùshì **héhū** dàodé**?**

Slide 3: How does one share work? … “Cloud” computing: You send the data to the “cloud”. The “Cloud” is a bunch of other computers and cell phones, etc. The others in the cloud do your calculations, and then “rain” down the answer.

第一個問題：你怎麼跟別的人一起做計算？**1** 我們用”Cloud Computing” (雲計算). 你發送你的數據到雲．那個雲是很多別的電腦跟手機，等等．**2**別的電腦在雲裡面做你的計算，**3** 之後**答案dá'àn**下雨回來.

Dì yī gè wèntí: Nǐ zěnme gēn bié de rén yīqǐ zuò jìsuàn? **1** Wǒmen yòng ”Cloud Computing” (yún jìsuàn). Nǐ fāsòng nǐ de shùjù dào yún. Nàgè yún shì hěnduō bié de diànnǎo gēn shǒujī, děng děng. **2** Bié de diànnǎo zài yún lǐmiàn zuò nǐ de jìsuàn, **3** zhīhòu dá'àn xià yǔ huílái.

Slide 4: However, there is still a problem: Can you trust others? Here is an idea: If you could send the data so that they could do the calculations but not see the data, then there is no problem. Can we “mess up” the data in some way so that they can’t read it? This question is hard, so we will return to it later.

但是，還有一個**擔心dānxīn**: **1** 你能不能**相信xiāngxìn**別的人？**2**如果**妳nǎi**會給那些雲的人你的數據**让ràng**他們可以做你想要的計算，但是看不到這個數據，那沒問題．**3**我們可以給他們**弄亂nòng luàn**的數據, 所以他們不能讀它. **4**請問:有没有可能無法看到數據，但**仍然réngrán**可以做計算呢？這個是很難的問題，所以我們稍**shāo**後會討論它．

Dànshì, hái yǒu yīgè **dānxīn**: **1** Nǐ néng bùnéng xiāngxìn bié de rén? **2** Rúguǒ **nǎi** huì gěi nàxiē yún de rén nǐ de shùjù **ràng** tāmen kěyǐ zuò nǐ xiǎng yào de jìsuàn, dànshì kàn bù dào zhège shùjù, nà méi wèntí. Wǒmen kěyǐ gěi tāmen **nòng luàn** de shùjù, suǒyǐ tāmen bùnéng dú tā. Qǐngwèn: Yǒu méiyǒu kěnéng wúfǎ kàn dào shùjù, dàn réngrán kěyǐ zuò jìsuàn ne? Zhège shì hěn nán de wèntí, suǒyǐ wǒmen shāo hòu huì tǎolùn tā.

Slide 5: Second question: Right now, the bank keeps track of your transactions and verifies your account balance. Suppose that you do not trust banks, and you want to collectively keep records on the internet. You want a decentralized system, and this is the idea of Bitcoin.

第二個問題：**1** 現在，銀行跟**蹤zōng**你的交易和**進行jìnxíng驗證yànzhèng**您的**帳戶zhànghù餘額yú'é**．**假設Jiǎshè**你不**相信xiāngxìn**銀行，那想要在**網wǎng**路上一起跟別的人**(保存bǎocún)**這些交易**紀錄jìlù**. 你想要一個去中心**化huà**的銀行. **2**  這就是”Bitcoin”的想法.

Dì èr gè wèntí: **1** Xiànzài, yínháng gēnzōng nǐ de jiāoyì hé jìnxíng yànzhèng nín de zhànghù yú'é. Jiǎshè nǐ bù xiāngxìn yínháng, nà xiǎng yào zài wǎng lùshàng yīqǐ gēn bié de rén (**bǎocún**) zhèxiē jiāoyì **jìlù**. Nǐ xiǎng yào yīgè qù zhōngxīn **huà** de yínháng. **2**  Zhè jiùshì”Bitcoin” de xiǎngfǎ.

Slide 6: In the implementation of Bitcoin, a transaction is sent and verified by a collective group of computers. Here validation is needed to check that the transaction really occurred. Then, once all of the computers agree, it is added to a new “block” of transactions which is then added to the “chain” of all transactions (this is the “Blockchain”). There is no central entity (like the bank) with the authority to change transactions. Transactions added to the “Blockchain” are unable to be changed. Nobody has the authority to decide to freeze your assets (banks sometimes freeze your money if they think you are doing something illegal), but nobody can correct mistakes, either (banks correct errors or thefts, for example). Cryptography is used in two main places in Cryptocurrency: Firstly, the transactions need to be verified. These are “signed” with a private key to verify your identity (otherwise people could steal your money by pretending to be you!). We will talk about private and public keys later. Secondly, blocks are put onto the “blockchain” by hashing the data from the previous block, which prevents someone adding a block invalidating all of the information.

為了**實現shíxiàn**”Bitcoin”, **1**  你的電腦發送一個交易到網路上(這就是“雲”/Cloud computing差不多一樣) , **2**一些電腦們**集體驗證jítǐ yànzhèng**這個交易. 我們**需xū**要這些**驗證yànzhèng**去**證實zhèngshí** ​​交易真的發生了. 那麼, 大家都同**意yì**之後, 交易被**放bèi fàng**入一個新的”block”(區塊); 然後這個新的”block”**被鏈接bèi liànjiē**到**由yóu**所有交易**構成gòuchéng**的**鏈liàn**上;這就是所謂的”blockchain” (區塊鏈).**3** Bitcoin/Blockchain没有中央**實體shítǐ**(銀行是**傳統chuántǒng**的交易中央)有**權限quánxiàn**去**更改gēnggǎi**交易, 所以**完成wánchéng**交易不能**被取消bèi qǔxiāo**.**4** 沒有中央的人可以**凍結dòngjié**你的**資產zīchǎn** (比如說有時候銀行會**凍結dòngjié**你的錢如果他們覺得juédé你在做**非法fēifǎ**的事情shìqíng)，但是也沒有人可以**糾**正**錯誤jiū**zhèng **cuòwù** (銀行會**糾jiū**正**錯cuò**的交易也可以回給你**贓款zāngkuǎn**). **實現Shíxiàn** ”Bitcoin” 的時候在兩個地方使用了密碼學：**5**　第一個：交易一定**驗證yànzhèng**了. 你的交易一定**簽qiān**名了： 你使用你密碼學的＂**私sī**鑰＂**簽qiān**名（**否則其**他**fǒuzé qí**tā人可以**假裝jiǎzhuāng**你**偷走tōu zǒu**你的錢）. 我們**稍shāo**後會討論密碼學的＂公鑰匙/**私sī**鑰匙”. 在做＂bitcoin”的時候第二個密碼學的用法：區塊**被**放**bèi** fàng在**鏈liàn**上的時候,新的數據一定跟前一個區塊的數據一起**散列sàn liè**，所以壞人不能加入一個新的區塊，使以前的數據**無效wúxiào**.

Wèile **shíxiàn**”Bitcoin”, **1**  nǐ de diànnǎo fāsòng yīgè jiāoyì dào wǎng lùshàng (Zhè jiùshì “yún”/Cloud computing chàbùduō yīyàng),**2** yīxiē diànnǎomen **jítǐ yànzhèng** zhège jiāoyì. Wǒmen **xū**yào zhèxiē **yànzhèng** qù **zhèngshí** jiāoyìzhēn de fǎ shēng le. Nàme, dàjiā dōu tóng**yì** zhīhòu, jiāoyì **bèi fàng** rù yīgè xīn de”block”(qū kuài); ránhòu zhège xīn de”block” **bèi liànjiē** dào **yóu** suǒyǒu jiāoyì **gòuchéng** de **liàn** shàng; zhè jiùshì suǒwèi de”blockchain” (qū kuài liàn).**3** Bitcoin/Blockchain méiyǒu zhòng yāng **shítǐ** (yínháng shì **chuántǒng** de jiāoyì zhōngyāng) yǒu **quánxiàn** qù **gēnggǎi** jiāoyì, suǒyǐ **wánchéng** jiāoyì bùnéng **bèi qǔxiāo**. Méiyǒu zhòng yāng de rén kěyǐ **dòngjié** nǐ de **zīchǎn** (bǐrú shuō yǒu shíhòu yínháng huì **dòngjié** nǐ de qián rúguǒ tāmen juédé nǐ zài zuò **fēifǎ** de shìqíng), dànshì yě méiyǒu rén kěyǐ **jiū**zhèng **cuòwù** (yínháng huì **jiū**zhèng **cuò** de jiāoyì yě kěyǐ huí gěi nǐ **zāngkuǎn**). **Shíxiàn** ”Bitcoin” de shíhòu zài liǎng gè dìfāng shǐyòngle mìmǎ xué: **5** Dì yīgè: Jiāoyì yīdìng **yànzhèng**le. Nǐ de jiāoyì yīdìng **qiān**míngle: Nǐ shǐyòng nǐ mìmǎ xué de"**sī** yào"qiānmíng (**fǒuzé qí**tā rén kěyǐ **jiǎzhuāng** nǐ **tōu zǒu** nǐ de qián). Wǒmen **shāo** hòu huì tǎolùn mìmǎ xué de"gōng yàoshi/**sī** yàoshi”. Zài zuò"bitcoin” de shíhòu dì èr gè mìmǎ xué de yòngfǎ: Qū kuài **bèi** fàng zài **liàn** shàng de shíhòu, xīn de shùjù yīdìng gēnqián yīgè qū kuài de shùjù yīqǐ **sàn liè**, suǒyǐ huàirén bùnéng jiārù yī gè xīn de qū kuài, shǐ yǐqián de shùjù **wúxiào**.

Slide 7: What is cryptography? How do you do cryptography? Can you safely send data? Can someone see what you’re doing? Can you trust them? After sending the data, can the recipient do the calculations you want, but still have the data stay safe?

甚麼是密碼學？你怎麼做密碼學？**1**可以安全發送數據嗎？**2**有壞人可能看到你發送的數據嗎？3你可不可以**相**信**xiāng**xìn他們？**4**數據發送的以後，接**jiē**收shōu數據的人可不可以做你想要的計算, 但是數據**保持bǎochí**安全呢？

Shénme shì mìmǎ xué? Nǐ zěnme zuò mìmǎ xué? Kěyǐ ānquán fāsòng shùjù ma? Yǒu huàirén kěnéng kàn dào nǐ fāsòng de shùjù ma? Nǐ kěbù kěyǐ **xiāng**xìn tāmen? Shùjù fāsòng de yǐhòu, **jiē**shōu shùjù de rén kěbù kěyǐ zuò nǐ xiǎng yào de **jìsuàn**, dànshì shùjù **bǎochí** ānquán ne?

Slide 8: Let’s begin with the question of how to do cryptography. The idea of modern cryptography is to find a “one-way function”, a math problem which is hard to solve, but easy to check if an answer is given to you.

**1**我們要開始想一想密碼學怎麼做了．**2**現**代dài**密碼學的中心**思sī**想是找到所謂的”one-way functions”; **3**一個”one-way function” 是一個很難的數學問題, 但是你**解決jiějué**那個數學問題以後，那別的人可以很容易**校驗jiào yàn**你的**解答jiědá**．**4**我們**稍shāo**後會看到”one-way function” 的例子．

Wǒmen yào kāishǐ xiǎng yī xiǎng mìmǎ xué zěnme zuòle. Xiàn**dài** mìmǎ xué de zhōngxīn **sī**xiǎng shì zhǎodào suǒwèi de”one-way functions”;**1** yīgè”one-way function” shì yīgè hěn nán de shùxué wèntí, dànshì nǐ **jiějué** nàgè shùxué wèntí yǐhòu, nà bié de rén kěyǐ hěn róngyì **jiào yàn** nǐ de **jiědá.** Wǒmen **shāo** hòu huì kàn dào”one-way function” de lìzi.

Slide 9: These questions are too hard to begin with, so let’s go back to the beginning and consider cryptography from the beginning, going back through history. You want to send an important message. You can give it to a courier, but can you trust the courier? What if someone intercepts it in between?

這些問題太難以開始了，所以我們要回到過去. 我們要**從cóng**開始學，學**習xí**密碼學的**歷史lìshǐ**．**1**你想要發送很**重zhòng**要的信息．**2**你可以**把bǎ**它給快**遞dì**，**3**但是不知道你會不會**相xiāng**信他／她．**4**如果有人在中間**攔截lánjié**它呢？

Zhèxiē wèntí tài nányǐ kāishǐle, suǒyǐ wǒmen yào huí dào guòqù. Wǒmen yào **cóng** kāishǐ xué, xué**xí** mìmǎ xué de **lìshǐ**. Nǐ xiǎng yào fāsòng hěn **zhòng**yào de xìnxī. Nǐ kěyǐ **bǎ** tā gěi kuài**dì**, dànshì bù zhīdào nǐ huì bù huì **xiāng**xìn tā. Rúguǒ yǒurén zài zhōngjiān **lánjié** tā ne?

Slide 10: We’ll start a long, long time ago

我們開始到很久以前．

Wǒmen kāishǐ dào hěnjiǔ yǐqián.

Slide 11: Caesar wanted to send a message, but he didn’t want his enemy to steal it. For example, maybe he’s coordinating an attack, and it would put him at a disadvantage if the enemy knew this information. Caesar’s solution: the “Caesar cipher”; every letter is “shifted” to another letter, 3, 5, or so to the right. But where does the letter ‘z’ go to? We use “clock arithmetic”.

Caesar 想要發送一個**重zhòng**要的信息，但是他不想**敵dí**人**攔截lánjié**它．例如，Caesar想要**協調攻擊xiétiáo gōngjí**．如果他的**敵dí**人知道他想要做的，那他會**失shī**去**戰鬥zhàndòu**. **1** Caesar的**解答jiědá**：所謂的”Caesar cipher”; **2**每一個字母都**被bèi**右**移yí**了三個，五個，等等字母．我們可以說”字母’a’ 加 三”等於字母‘d’. 請問：字母’z’**被放bèi fàng**到哪裡了？我們使用所謂的”clock arithmetic” (時鐘**算術suànshù**；也可以說”modular arithmetic”）．

Caesar xiǎng yào fāsòng yīgè **zhòng**yào de xìnxī, dànshì tā bùxiǎng **dí**rén **lánjié** tā. Lìrú, Caesar xiǎng yào **xiétiáo gōngjí**. Rúguǒ tā de **dí**rén zhīdào tā xiǎng yào zuò de, nà tā huì **shī**qù **zhàndòu**. Caesar de **jiědá**: Suǒwèi de”Caesar cipher”; měi yīgè zìmǔ dōu **bèi** yòu **yí**le sān gè, wǔ gè, děng děng zìmǔ. Wǒmen kěyǐ shuō” zìmǔ’a’ jiā sān” děngyú zìmǔ ‘d’. Qǐngwèn: Zìmǔ’z’ **bèi fàng** dào nǎlǐle? Wǒmen shǐyòng suǒwèi de”clock arithmetic” (shízhōng **suànshù**; Yě kěyǐ shuō ”modular arithmetic”).

Slide 12: On a clock, 1 o’clock and 13 o’clock are the same. When doing Caesar ciphers we do the same thing. In other words, ‘z’ plus 3 equals ‘c’. If a clock has 24 hours, then one o’clock and 13 o’clock are not the same, but one o’clock and 25 o’clock are still the same. What if a clock had 26 hours (like the 26 letters in the English alphabet)? Or 7 hours? Or 11 hours?

**1**在時鐘上，一點跟十三點一樣了．做”Caesar cipher”的時候, 我們做一樣的事情：”字母’z’ 加三”等於字母’c’.**2**如果時鐘有二十四小時, 那一點跟十三點就不一樣了，但是一點跟二十五點還是一樣的.**3** 如果時鐘有二十六小時(和英文字母的數**量liàng**一樣)呢？**或者Huòzhě**七個小時呢? **或者Huòzhě**十一個小時呢?

Zài shízhōng shàng, yīdiǎn gēn shísān diǎn yīyàngle. Zuò”Caesar cipher” de shíhòu, wǒmen zuò yīyàng de shìqíng:” Zìmǔ’z’ jiā sān” děngyú zìmǔ’c’. Rúguǒ shízhōng yǒu èrshísì xiǎoshí, nà yīdiǎn gēn shísān diǎn jiù bù yīyàngle, dànshì yīdiǎn gēn èrshíwǔ diǎn háishì yīyàng de. Rúguǒ shízhōng yǒu èrshíliù xiǎoshí (hé yīngwén zìmǔ de shù**liàng** yī yàng) ne? **Huòzhě** qī gè xiǎoshí ne? **Huòzhě** shíyī gè xiǎoshí ne?

Slide 13: Let’s try some modular arithmetic. If a clock has 8 hours and starts at 7 o’clock and runs for two hours, when does it end (what time does the clock say?)? Seven plus 2 is nine, so .. it says one o’clock on the clock. We say that 7+2 and 1 are „congruent modulo 8“ if they „have the same time“ on an 8-hour clock.

**1**我們算算看,做”modular arithmetic”.**2**如果時鐘有八個小時,**3** 你開始上課的時間是七點, 上課兩個小時, 那這個課甚麼時候**結束jiéshù**了(甚麼時間在時鐘上了?)? **4**七加二等於九, 所以…**5** 一點在時鐘上. 因為九跟一在八個小時的時鐘在一樣的**位置zhì**,所以我們說七加二(等於九) 跟一是”congruent modulo” 八.我們寫七加二”is congruent to”一(“mod” 八).

Wǒmen suàn suàn kàn, zuò”modular arithmetic”. Rúguǒ shízhōng yǒu bā gè xiǎoshí, nǐ kāishǐ shàngkè de shíjiān shì qī diǎn, shàngkè liǎng gè xiǎoshí, nà zhège kè shénme shíhòu **jiéshù**le (shénme shíjiān zài shízhōng shàngle?)? Qī jiā èr děngyú jiǔ, suǒyǐ… yīdiǎn zài shízhōng shàng. Yīnwèi jiǔ gēn yī zài bā gè xiǎoshí de shízhōng zài yīyàng de wèi**zhì**, suǒyǐ wǒmen shuō qī jiā èr (děngyú jiǔ) gēn yī shì”congruent modulo” bā. Wǒmen xiě qī jiā èr”is congruent to” yī (“mod” bā).

Slide 14: Here’s the next example. Every non-leap year has 365 days. Last year, your birthday was on a Wednesday. Every week has 7 days. Three hundred sixty-four is 52 times 7; the remainder equals one, so there is a shift of one day, and your birthday will be on Thursday this year.

**1**下一個例子: **2**每一個**非閏fēi rùn**年有三百六十五天. **3**如果你去年的生日在星期三, 那今年的生日**將jiàng**在一周zhōu中的哪一天? **4**每周有七天. **5**三百六十四等於七**乘chéng**以五十二; **6餘yú**數等於一, 所以你生日轉**移**zhuǎn**yí**了一天. 那你今年的生日**將jiàng**在…**7**星期四.

Xià yīgè lìzi: Měi yīgè **fēi rùn**nián yǒu sānbǎi liùshíwǔ tiān. Rúguǒ nǐ qùnián de shēngrì zài xīngqísān, nà jīnnián de shēngrì **jiàng** zài yīzhōu zhōng de nǎ yītiān? Měi zhōu yǒu qītiān. Sānbǎi liùshísì děngyú qī **chéng** yǐ wǔshí'èr; **yú**shù děngyú yī, suǒyǐ nǐ shēngrì zhuǎn**yí**le yītiān. Nà nǐ jīnnián de shēngrì **jiàng** zài…xīngqísì.

Slide 15: Can you solve the following congruences? Give it a try.

**1**你可不可以**解決jiějué**以下的問題? 你試試看! … 第一個問題: x 等於零. 第二個問題: x 等於二. 第三個問題: x 等於六.

Nǐ kěbù kěyǐ **jiějué** yǐxià de wèntí? Nǐ shì shìkàn! … Dì yī gè wèntí: X děngyúlíng. Dì èr gè wèntí: X děngyú èr. Dì sān gè wèntí: X děngyú liù.

Slide 16: Ok. Since you are now comfortable with modular arithmetic, let’s try to encrypt a message. We choose a shift of 10. The original message is “attack at midnight”. We first convert every letter to a number. Then we add 10 to each number and convert back into letters. We finally send “lddlnu ld wsnxsqrd” (we take out the spaces when we send it). The recipient reverses these steps. In practice, a ring which matched the beginning and ending letters was used to do the encoding/decoding. This is where the term “decoder ring” comes from.

好了. 因為你們現在習慣xíguàn了”modular arithmetic”, 所以我們可以使用一個”Caesar Cipher”為一個信息加密做做看. **1**我們要每個字母**被bèi**右**移yí**了十個字母. **2**Caesar的**原始yuánshǐ**信息是”attack at midnight”. 第一步:**3** 我們**將jiāng**每個字母轉**換huàn**為數字. 下一步: 每個數字要加十, 然後轉換回到字母. 最後, 我們發送的是**4**”kddkmu kd wsnxsqrd”(發送的時候, 我們**刪除shānchú**空**格**kòng**gé**). **5**收**件jiàn**人**反轉fǎn zhuǎn**了這些步**驟zhòu**. 在**實踐shíjiàn**中，他們使用一個**匹配pǐpèi**原始和**結束jiéshù**字母的**旋轉**還xuánzhuǎn hái .這是”decoder ring”的來**源yuán.**

Hǎole. Yīnwèi nǐmen xiànzài xíguànle”modular arithmetic”, suǒyǐ wǒmen kěyǐ shǐyòng yīgè”Caesar Cipher” wéi yīgè xìnxī jiāmì zuò zuò kàn. Wǒmen yào měi gè zìmǔ **bèi** yòu **yí**le shí gè zìmǔ. Caesar de **yuánshǐ** xìnxī shì”attack at midnight”. Dì yībù: Wǒmen **jiāng** měi gè zìmǔ zhuǎn**huàn** wéi shùzì. Xià yī bù: Měi gè shùzì yào jiā shí, ránhòu zhuǎnhuàn huí dào zìmǔ. Zuìhòu, wǒmen fāsòng de shì”lddlnu ld wsnxsqrd”(fāsòng de shíhòu, wǒmen **shānchú** kònggé). Shōu **jiàn** rén **fǎn zhuǎn**le zhèxiē bùzhòu. Zài **shíjiàn** zhōng, tāmen shǐyòng yīgè **pǐpèi** yuánshǐ hé **jiéshù** zìmǔ de xuánzhuǎn hái. Zhè shì”decoder ring” de lái**yuán**.

Slide 17: Let’s try an easier example and do it ourselves. The secret message is “hi”. ‘h’ is 8, ‘i’ is 9. We then add 20 to each number. What do we send? Try it yourself. … You send …

**1**我們現在自己做一個容易的例子试试看. **2**我們**秘**密**mì**mì的消息是”hi”.**3** 字母’h’等於八號, 字母’i’等於九號.然後, 每一個數字要加二十, **4**所以我們有二十八跟二十九. 最後, 我們發送的是甚麼? **5**你自己试试看. **6**你發送的是: … **7**“bc”.

Wǒmen xiànzài zìjǐ zuò yīgè róngyì de lìzi shì shìkàn. Wǒmen **mì**mì de xiāoxī shì”hi”. Zìmǔ'h'děngyú bā hào, zìmǔ'i'děngyú jiǔ hào. Ránhòu, měi yīgè shùzì yào jiā èrshí, suǒyǐ wǒmen yǒu èrshíbā gēn èrshíjiǔ. Zuìhòu, wǒmen fāsòng de shì shénme? Nǐ zìjǐ shì shìkàn. Nǐ fāsòng de shì: … “bc”.

Slide 18: Here’s another secret message. Can you decode his message? … It is harder without knowing the shift. Since you came to my talk, I’ll give you the secret information.

現在,我們看另一個秘密消息. **1**你會不會**解碼jiěmǎ**這**條tiáo**消息呢? … 如果你不知道轉**移yí**多遠yuǎn, 那很難. 因為你們來這裡看過我的**演講yǎnjiǎng**, **2**所以我給你這祕密的信息. … … 我寫一個小的會給我們這個答案的電腦**程序chéngxù.** … 它就是“rambling in maths“**.**

Xiànzài, wǒmen kàn lìng yīgè mìmì xiāoxī. Nǐ huì bù huì **jiěmǎ** zhè **tiáo** xiāoxī ne? … Rúguǒ nǐ bù zhīdào zhuǎn**yí** duō yuǎn, nà hěn nán. Yīnwèi nǐmen lái zhèlǐ kànguò wǒ de **yǎnjiǎng**, suǒyǐ wǒ gěi nǐ zhè mìmì de xìnxī. … … Wǒ xiě yīgè xiǎo de huì gěi wǒmen zhège dá'àn de diànnǎo**chéngxù**. … Tā jiùshì “rambling in maths“

Slide 19: Caesar’s code has a problem. What happens if someone steals the data? They could try to guess the shift. If they guess correctly, they will know it, because they can read the text. How can one guess? Some English letters occur more often, so you can find the most frequent letters and guess that these are ‘d’, ‘t’, or ‘e’. Maybe you can just replace letters instead? But then one can still guess based on frequency.

“Caesar cipher” 有一個問題. **1**如果有人**竊取qièqǔ**你的信息,**2** 那麼他們可以**猜測cāicè**你轉移zhuǎnyí了多遠yuǎn. **3**如果他們**猜cāi**對了,他們就知道信息的**内容nèiróng**了，因為他們可以讀dú到文本. 怎麼可以猜猜看了呢?**4** 因為英文有常常使用的字母, 所以你會找到在信息裡面使用最多的字母, 然後猜猜這個字母是字母'd’, 字母’t’, 還是字母’e’. **5**另一個想法: 你只要做一個字母匹配. **6**但人們還可以**根據gēnjù**常常使用的字母**猜測cāicè**它.

“Caesar cipher” yǒu yīgè wèntí. Rúguǒ yǒurén **qièqǔ** nǐ de xìnxī, nàme tāmen kěyǐ **cāicè** nǐ zhuǎnyíle duō yuǎn. Rúguǒ tāmen **cāi** duìle, tāmen jiù zhīdào xìnxī de **nèiróng**le, yīnwèi tāmen kěyǐ dú dào wénběn. Zěnme kěyǐ cāi cāi kànle ne? Yīnwèi yīngwén yǒu chángcháng shǐyòng de zìmǔ, suǒyǐ nǐ huì zhǎodào zài xìnxī lǐmiàn shǐyòng zuìduō de zìmǔ, ránhòu cāi cāi zhège zìmǔ shì zìmǔ'd', zìmǔ't', háishì zìmǔ'e'. Lìng yīgè xiǎngfǎ: Nǐ zhǐyào zuò yīgè zìmǔ pǐpèi. Dàn rénmen hái kěyǐ **gēnjù** chángcháng shǐyòng de zìmǔ **cāicè** tā.

Slide 20: Another attempt: make a random matching of letters. The Spartans wrapped leather containing letters around a long rod. If the width of the rod was correct, it spelled a word, but if the width was incorrect, then it wouldn’t make sense. People can still attack these methods by looking for the most common letters, though.

另外一個例子用不同的方法加密: **1隨機進Suíjī jìn**行字母的匹配. **2**“Spartan” 的**軍隊jūnduì**使用長的**竿gān**, 在它**周圍zhōuwéi**包上**皮革****pígé. 皮革Pígé**上有字母. 如果你的**竿gān**有正**確què**的寬度kuāndù,那麼你可以**閱****yuè**讀這個信息. 如果寬度kuāndù不對, 就不能**閱yuè**讀它. **3**但是,壞人還是可以**計**算字母**頻率pínlǜ**.

Lìngwài yīgè lìzi yòng bùtóng de fāngfǎ jiāmì: **Suíjī jìn**xíng zìmǔ de pǐpèi. “Spartan” de**jūnduì** shǐyòng cháng de **gān**, zài tā **zhōuwéi** bāo shàng **pígé**. **Pígé** shàng yǒu zìmǔ. Rúguǒ nǐ de**gān** yǒu zhèng**què** de kuāndù, nàme nǐ kěyǐ **yuè**dú zhège xìnxī. Rúguǒ kuāndù bùduì, jiù bùnéng **yuè**dú tā. Dànshì, huàirén háishì kěyǐ jìsuàn zìmǔ **pínlǜ**.

Slide 21: Let’s try something different.

我們來試試另外一個.

Wǒmen lái shì shì lìngwài yīgè.

Slide 22: We’ve discussed the problems with random replacement/matching. Does every letter always have to go to the same letter, though? Maybe we could have multiple choices for each letter to be changed to. The “Grand Chiffre” in the royal court of France changed syllables to multiple choices of other similar-sounding syllables.

**1隨機Suíjī**匹配的問題我們已經yǐjīng**討論tǎolùn**了.**2**但是一個字母一定要每次**轉換****zhuǎnhuàn**到一樣的字母嗎?**3** 也**許xǔ**每個字母有可能有很多**選擇xuǎnzé**來**轉換zhuǎnhuàn**它. **4**法國**宮廷gōngtíng**使用的”Grand Chiffre”**將jiāng**每個**音節yīnjié**(**5**它不是字母**轉換****zhuǎnhuàn**的密碼**系統**mìmǎ **xìtǒng**) 轉換**zhuǎnhuàn**成多個**聲**音**shēngyīn**差不多一樣的音節yīnjié.**6**

**Suíjī** pǐpèi de wèntí wǒmen yǐjīng **tǎolùn**le. Dànshì yīgè zìmǔ yīdìng yào měi cì zhuǎnhuàn dào yīyàng de zìmǔ ma? Yě**xǔ** měi gè zìmǔ yǒu kěnéng yǒu hěnduō **xuǎnzé** lái **zhuàn huàn** tā. Fàguó **gōngtíng** shǐyòng de”Grand Chiffre”**jiāng** měi gè **yīnjié** (tā bùshì zìmǔ **zhuǎnhuàn** de mìmǎ **xìtǒng**) zhuǎnhuàn **chéng** duō gè **shēngyīn** chàbùduō yīyàng de **yīnjié**.

Slide 23: Why is this better? Guessing is harder, … and frequent letters/syllables get shared among more choices. Do new problems arise? Every letter has many possible outputs, so you need to know when to switch. If ‘a’ and ‘b’ both sometimes go to ‘e’, then how does the receiver decide if an ‘e’ is really an ‘a’ or a ‘b’? “Caesar cipher” didn’t have this problem because the change was unique. If you use a simple method to change choices, then people in the middle can also figure it out.

**1**這個密碼**系統**為甚麼比”Caesar cipher”更好了? 在這個密碼**系統**,壞人猜cāi對字母更難… 常常使用的字母(還有**音節yīnjié**)也在**許****xǔ**多**選擇****xuǎnzé**中**共享gòngxiǎng**. 但是這個密碼**系統**有新的問題嗎? **2**因為每個字母有**許xǔ**多**選擇xuǎnzé**,所以你一定要知道**何hé**時**切換選擇qiēhuàn xuǎnzé**. 如果字母'a'和字母'b'都**轉換zhuǎnhuàn**到'e'了, 那麼收信息的人怎麼**決jué**定這個在**轉換zhuǎnhuàn**信息中的' e'在**原版yuánbǎn**的信息中是'a'還是'b'? 因為“Caesar cipher” **換**有**唯wéi**一的**轉zhuǎnhuàn**,所以它沒有這個問題. 如果你用容易的方法來**決jué**定甚麼時候**轉huàn**別的**選擇xuǎnzé**,那麼壞人在中間也會知道你**轉huàn**別的**選擇xuǎnzé**.

Zhège mìmǎ **xìtǒng** wéishènme bǐ”Caesar cipher” gèng hǎole? Zài zhège mìmǎ xìtǒng, huàirén cāi duì zìmǔ gèng nán… chángcháng shǐyòng de zìmǔ (hái yǒu **yīnjié**) yě zài **xǔ**duō **xuǎnzé** zhōng **gòngxiǎng**. Dànshì zhège mìmǎ xìtǒng yǒu xīn de wèntí ma? Yīnwèi měi gè zìmǔ yǒu **xǔ**duō **xuǎnzé**, suǒyǐ nǐ yīdìng yào zhīdào **hé**shí**qiēhuàn xuǎnzé**. Rúguǒ zìmǔ’a’ hé zìmǔ’b’ dōu **zhuǎnhuàn** dào’e’ le, nàme shōu xìnxī de rén zěnme **jué**dìng zhège zài **zhuǎnhuàn** xìnxī zhōng de’e’ zài **yuánbǎn** de xìnxī zhōng shì’a’ háishì’b’? Yīnwèi “Caesar cipher” yǒu **wéi**yī de **zhuǎnhuàn**, suǒyǐ tā méiyǒu zhège wèntí. Rúguǒ nǐ yòng róngyì de fāngfǎ lái **jué**dìng shénme shíhòu **huàn** bié de **xuǎnzé**, nàme huàirén zài zhōngjiān yě huì zhīdào nǐ **huàn** bié de **xuǎnzé**.

Slide 24: This type of cryptosystem is called a “polycipher”. One example of a polycipher is a repetitive usage of Caesar cipher. In this system, the first letter is shifted a certain number of places, then the next is shifted another number of places, and so on. For example, we can shift 3 spaces, then 11 spaces, then 5 spaces, and repeat. Let’s try this with the original message “Here is a message”. The encrypted message is “kpwhtxdxjvdfjp”. The original message has a lot of ‘e’s, but they are distinct in the encrypted message. We therefore conclude that it is better than the “Caesar cipher”. However, people in the middle can guess the length of the repeating period of the shifts, and then they can again do frequency counts to attack this cipher just like “Caesar cipher”.

使用**許xǔ**多轉**換huàn**的密碼**系統xìtǒng**叫”polycipher”. **1**一個例子是多次使用”Caesar cipher”. 在這個”polycipher”裡,第一個字母要轉**移**zhuǎn**yí**右幾個**位置wèizhì**,然後下一個字母要轉**移**zhuǎn**yí**右不同數**量liàng**的**位置wèizhì**, 等等. 例如, 第一個字母有可能轉**移**zhuǎn**yí**右三個**位置wèizhì**, 第二個字母轉**移**zhuǎn**yí**右十一個**位置wèizhì**, 第三個字母轉**移**zhuǎn**yí**右五個**位置wèizhì**, 之後我們**重複chóngfù**這些轉**移**zhuǎn**yí**的長度dù. 現在我們的**原始yuánshǐ**信息是**2**”Here is a message”， 我們用這個密碼**系統xìtǒng**做做看. ‘h’ 轉**換huàn**到’k’, ‘e’ 轉**換huàn**到’p’, 等等… **3**加密的消息是”kpwhtxdxjvdfjp”. **原始Yuánshǐ**的信息有很多字母'e', 但是在加密的消息中它們是不同的.**因此Yīncǐ**我們看到它比”Caesar cipher”更好. **4然而Rán'ér**, 如果中間的人可以**猜測cāicè**我們用的**重複週期chóngfù****zhōuqí**的長度, 那麼他們還可以找到常常使用的字母（然後,這個密碼**系統**有可能**受shòu**到跟”Caesar cipher ”同樣方**式shì**的**攻擊gōngjí**）.

Shǐyòng **xǔ**duō zhuǎn**huàn** de mìmǎ**xìtǒng** jiào”polycipher”. Yīgè lìzi shì duō cì shǐyòng”Caesar cipher”. Zài zhège”polycipher” lǐ, dì yīgè zìmǔ yào zhuǎn**yí** yòu jǐ gè **wèizhì**, ránhòu xià yī gè zìmǔ yào zhuǎn**yí** yòu bùtóng shù**liàng** de **wèizhì**, děng děng. Lìrú, dì yī gè zìmǔ yǒu kěnéng zhuǎn**yí** yòu sān gè **wèizhì**, dì èr gè zìmǔ zhuǎn**yí** yòu shíyī gè **wèizhì**, dì sān gè zìmǔ zhuǎn**yí** yòu wǔ gè **wèizhì**, zhīhòu wǒmen **chóngfù** zhèxiē zhuǎn**yí** de chángdù. Xiànzài wǒmen de **yuánshǐ** xìnxī shì”Here is a message”, wǒmen yòng zhège mìmǎ **xìtǒng** zuò zuò kàn. ‘h’ zhuǎnhuàn dào’k’, ‘e’ zhuǎnhuàn dào’p’, děng děng… Jiāmì de xiāoxī shì”kpwhtxdxjvdfjp”. **Yuánshǐ** de xìnxī yǒu hěnduō zìmǔ’e’, dànshì zài jiāmì de xiāoxī zhōng tāmen shì bùtóng de. **Yīncǐ** wǒmen kàn dào tā bǐ”Caesar cipher” gèng hǎo. **Rán'ér**, rúguǒ zhōngjiān de rén kěyǐ **cāicè** wǒmen yòng de **chóngfù** **zhōuqí** de chángdù, nàme tāmen hái kěyǐ zhǎodào chángcháng shǐyòng de zìmǔ (ránhòu, zhège mìmǎ **xìtǒng** yǒu kěnéng **shòu**dào gēn”Caesar cipher” tóngyàng fāng**shì** de **gōngjí)**.

Slide 25: Let’s move to cryptography in more recent times.

我們現在討論更近期的密碼學．

Wǒmen xiànzài tǎolùn gèng jìnqí de mìmǎ xué.

Slide 26: The next attempt is to try to make too many choices for guessing to work. An example was Germany’s “Enigma” machine. This was an automated machine that changed the output each time that you put in an input. Therefore, each letter would have a different output each time that you entered it.

下一次**嘗試chángshì**：**1**我們使用很多的**選擇讓xuǎnzé ràng**人**無wú**法猜測cāicè.一個以前的例子是德國的”Enigma machine”. **2**這是一個自動的密碼機. 在這個機**器qì**裡面, 有**旋xuán**轉的**齒輪chǐlún**. **3**因為你每次按到一個字母 它的**齒輪chǐlún**要**旋xuán**轉, 所以每次按àn到一樣的字母 有可能不同的字母出來了.

Xià yīcì **chángshì**: Wǒmen shǐyòng hěn duō de **xuǎnzé ràng** rén **wú**fǎ cāicè. Yīgè yǐqián de lìzi shì déguó de”Enigma machine”. Zhè shì yīgèzìdòng de mìmǎ jī. Zài zhège jī**qì** lǐmiàn, yǒu **xuán**zhuǎn de **chǐlún**. Yīnwèi nǐ měi cì àn dào yīgè zìmǔ tā de **chǐlún** yào **xuán**zhuǎn, suǒyǐ měi cì àn dào yīyàng de zìmǔ yǒu kěnéng bùtóng de zìmǔ chūláile.

Slide 27: How does an Enigma machine work? First, you hit a key on the keyboard. The letter on this key is matched to another letter via a plugboard (the plugboard has one matching that never changes). Then this letter is matched to another one on the first rotor, which is in turn connected to a letter on the second rotor, and finally this letter is connected to another letter on the third rotor. Then the output is matched with another letter on a reflector (this is essentially the same as the plugboard). After this, it comes back through the rotors again. The rotors turn in the same way as adding with carry.

“Enigma machine” 是如何工作的呢? 開始的時候, 你按一個**鍵盤鍵** **jiànpán jiàn**.**１ 通Tōng**過一個**插件板chājiàn bǎn,**這個**鍵盤鍵** **jiànpán jiàn**上的字母與另外一個字母匹配 (這個**插件板**的匹配是**固gù**定的). **2**然後, 這個字母與第一個轉子上的另外一個字母**相xiāng**匹配. 第一個轉子上的字母與第二個轉子上的另外一個字母**相xiāng**匹配, 然後它與第三個轉子上的另外一個字母**相xiāng**匹配. **3**下一步**,** 這個**輸shū**出的字母與**反射板fǎnshè bǎn**上的另外一個字母**相xiāng**匹配 (這個**反射板fǎnshè bǎn**和**插件板chājiàn bǎn**做的事情差不多一樣). **4**然後, **輸shū**出的字母**又通yòu tōng**過轉子回來了.**5** 最後, 第一個轉子**旋轉xuánzhuǎn**了.**6** 它**旋轉xuánzhuǎn**第二十六個字母以後, 那第二個轉子也**旋轉xuánzhuǎn**了, 第二個轉子**旋轉xuánzhuǎn**第二十六個字母的時候, 第三個轉子也**旋轉xuánzhuǎn**了. 這就是帶**進**位**jìn**wèi加法的方法.

“Enigma machine” shì rúhé gōngzuò de ne? Kāishǐ de shíhòu, nǐ àn yīgè **jiànpán jiàn.** **Tōng**guò yīgè**chājiàn bǎn**, zhège **jiànpán jiàn** shàng de zìmǔ yǔ lìngwài yīgè zìmǔ pǐpèi (zhège **chājiàn bǎn** de pǐpèi shì **gù**dìng de). Ránhòu, zhège zìmǔ yǔ dì yīgè zhuànzǐ shàng de lìngwài yīgè zìmǔ **xiāng** pǐpèi. Dì yīgè zhuànzǐ shàng de zìmǔ yǔ dì èr gè zhuànzǐ shàng de lìngwài yīgè zìmǔ xiāng pǐpèi, ránhòu tā yǔ dì sān gè zhuànzǐ shàng de lìngwài yī gè zìmǔ xiāng pǐpèi. Xià yībù, zhè ge**shū**chū de zìmǔ yǔ **fǎnshè bǎn** shàng de lìngwài yī gè zìmǔ xiāng pǐpèi (zhège **fǎnshè bǎn** hé **chājiànbǎn** zuò de shìqíng chàbùduō yīyàng). Ránhòu, **shū**chū de zìmǔ **yòu tōng**guò zhuànzǐ huíláile. Zuìhòu, dì yī gè zhuànzǐ xuánzhuǎnle. Tā xuánzhuǎn dì èrshíliù gè zìmǔ yǐhòu, nà dì èr gè zhuànzǐ yě xuánzhuǎnle, dì èr gè zhuànzǐ xuánzhuǎn dì èrshíliù gè zìmǔ de shíhòu, dì sān gè zhuànzǐ yě xuánzhuǎnle. Zhè jiùshì dài **jìn** wèi jiāfǎ de fāngfǎ.

Slide 28: The process is symmetrical because of the reflector. Hence to decrypt, one only needs to set the rotors to the same starting position and then type the encrypted message into the machine. Because of this symmetry, the Germans constructed the “Enigma machine” so that it would never match a letter back to itself.

**1**因為**反射板fǎnshè bǎn,** 這個**過程guòchéng**是對**稱chèn**的.**1** 因此, 你想要**解碼jiěmǎ**加密的消息, 只**需xū**要用一個一**模mú**一樣旋轉xuánzhuǎn轉子**設置shèzhì**的機**器qì, 把bǎ**加密的消息**輸shū**入機**器qì. 2**因為”Enigma”**具jù**有這種zhǒng對**稱chèn**性**,** 德國**構建gòujiàn**它時，使字母不能自己匹配.

Yīnwèi **fǎnshè bǎn**, zhège **guòchéng** shì duì**chèn** de. Yīncǐ, nǐ xiǎng yào **jiěmǎ** jiāmì de xiāoxī, zhǐ **xū**yào yòng yīgè yīmú yīyàng xuánzhuǎn zhuànzǐ **shèzhì** de jī**qì**, **bǎ** jiāmì de xiāoxī **shū**rù jī**qì**. Yīnwèi”Enigma” **jù**yǒu zhè zhǒng duì**chèn**xìng, déguó **gòujiàn** tāshí, shǐ zìmǔ bùnéng zìjǐ pǐpèi.

Slide 29: Enigma was eventually broken by finding the rotor settings with the help of automation (many different possibilities were guessed simultaneously). But checking all possibilities with brute force would have been impossible (there are too many possibilities). One of the reasons Enigma was eventually broken were based on the symmetries, which reduced the number of possibilities. Not allowing a letter to be matched to itself reduced the number of possible choices, correct guesses reduce the choices further, and combining this with other symmetries allowed the British to reduce the number of possible choices to something that they could handle. They also used common signals sent by the Germans to look for patterns and test their guesses, working backwards.

最**終zhōng**,英國人打**破pò**了”Enigma”的加密. 他們用自動的機**器qì**猜到”Enigma”轉子的**設置shèzhì** (那個自動機會同時猜測很多轉子**設置shèzhì**的可能**性xìng**). 但是, 因為”Enigma” 有太多**設置shèzhì**的可能**性xìng**, 所以他們不能**試圖shìtú**猜測每一個轉子**設置shèzhì**. **2**他們打**破pò**”Enigma”的 一個**原**因**yuán**yīn是它的對**稱性**duì**chèn xìng**. 因為它有對**稱性**duì**chèn xìng**, 所以轉子**設置shèzhì**的可能**性xìng減jiǎn**少**.** **3**因為一個字母不能自己匹配, 所以可能**性xìng**也會**減jiǎn**少. 正**確**Zhèng**què**的**猜測cāicè**可以**進jìn**一步**減jiǎn**少**設置shèzhì**的可能**性xìng**. **4**英國人用這個方法**減jiǎn**少他們**猜測cāicè**的可能**性xìng**. **5**他們也知道德國每天發送的信息, 所以他們也會**測試cèshì**他們的猜測cāicè**並bìng向xiàng**後工作.

Zuì**zhōng**, yīngguó rén dǎ**pò**le”Enigma” de jiāmì. Tāmen yòng zìdòng de jī **qì**cāi dào”Enigma” zhuànzǐ de **shèzhì** (nàgè zìdòng jīhuì tóngshí cāicè hěnduō zhuànzǐ **shèzhìde** kěnéng **xìng**). Dànshì, yīnwèi”Enigma” yǒu tài duō **shèzhì** dekěnéng **xìng**, suǒyǐ tāmen bùnéng **shìtú** cāicè měi yīgè zhuànzǐ **shèzhì**. tāmen dǎ**pò**”Enigma” deyīgè yuányīn shì tā de duì**chèn xìng**. Yīnwèi tā yǒu duì**chèn xìng,** suǒyǐ zhuànzǐ **shèzhì** dekěnéng **xìng jiǎn** shǎo. Yīn wéi yīgè zìmǔ bùnéng zìjǐ pǐpèi, suǒyǐ kěnéng **xìng** yě huì **jiǎn**shǎo. Zhèng**què** de cāicè kěyǐ **jìn**yībù **jiǎn**shǎo **shèzhì** de kěnéng **xìng**. Yīngguó rén yòng zhège fāngfǎ **jiǎns**hǎo tāmen cāicè de kěnéng **xìng**. Tāmen yě zhīdào déguó měitiān fāsòng de xìnxī, suǒyǐ tāmen yě huì **cèshì** tāmen de cāicè **bìng xiàng**hòu gōngzuò.

Slide 30: Automated machines for encryption and decryption brought about major changes in cryptography.

可以加密與**解密jiěmì**的自動機器给密碼學帶來了很多**改變gǎibiàn**.

Kěyǐ jiāmì yǔ **jiěmì** de zìdòng jī qi gei mìmǎ xuédài lái le hěnduō**gǎibiàn**.

Slide 31: When constructing the Enigma machine, the Germans didn’t expect others to use an automated search. They made some choices which would not have been best with automated searches. Why? Computers search differently than humans

**1**德國**設計shèjì**”Enigma”的時候, 他們沒想到對手duìshǒu會使用自動的機**器qì**找得到轉子**設置shèzhì**的可能**性xìng**. 如果他們知道別的人用自動機找到轉子**設置shèzhì**的可能**性xìng,** 他們會**設計shèjì**不一樣的“Enigma”. 為甚麼?**2** 電腦找到的方法和人**類lèi**找到的方法不一樣. **3**這就是電腦**科學kēxué**的開**端duān**.電腦**科學kēxué**開始的時候, 他們真的在數學**系xì**做工作. **4**現在他們有自己的**系xì**.**5** 因為電腦和人**類**rén**lèi搜索sōusuǒ**的方法不同, 所以密碼學也一定**改變gǎibiàn**.

Déguó **shèjì**”Enigma” de shíhòu, tāmen méi xiǎngdào duìshǒu huì shǐyòng zìdòng de jī**qì** zhǎo dédào zhuànzǐ **shèzhì** dekěnéng **xìng**. Rúguǒ tāmen zhīdào bié de rén yòng zìdòng jī zhǎodào zhuànzǐ **shèzhì** dekěnéng **xìng**, tāmen huì **shèjì** bù yīyàng de“Enigma”. Wéishènme? Diànnǎo zhǎodào de fāngfǎ hé rén**lèi** zhǎodào de fāngfǎ bù yīyàng. Zhè jiùshì diànnǎo **kēxué** de kāi**duān**. Diànnǎo kēxué kāishǐ de shíhòu, tāmen zhēn de zài shùxué **xì** zuò gōngzuò. Xiànzài tāmen yǒu zìjǐ de**xì** . Yīnwèi diànnǎo hé rén**lèi sōusuǒ** de fāngfǎ bùtóng, suǒyǐ mìmǎ xué yě yīdìng **gǎibiàn**.

Slide 32: The advent of computers brought about a new method of cryptography. The basic idea is to find a mathematical operation which is easy to do in one direction, but hard to do in reverse. The operation is encryption, while the reverse is the decryption. Of course, it needs to be possible to do the decryption (reverse direction) with extra secret information. Here is an example: If you multiply 3571 and 6997, you can follow an easy series of steps (we all learned this is school, and computers are even better at this than us) and get 24986287. On the other hand, if I only give you the number 24986287, then can you find the original two numbers? If I give you one of the numbers, then you can find the other, but without either number it is hard to find them.

電腦的出現chūxiàn帶來了新的密碼學方法．他們新的想法如下：**1**找到一個數學**運算yùnsuàn**你可以容易做, 但是**顛倒diāndǎo**這個**運算yùnsuàn**很難.**2** 你想要加密的時候, 你做這個**運算yùnsuàn**.你想要**解密jiěmì**的時候, 你要**顛倒diāndǎo**它. **當然Dāngrán**, 你的朋友可能能**夠**néng**gòu逆**轉**nì**zhuǎn這個**運算yùnsuàn**.**3** 如果他們知道**秘密mìmì, 反向fǎn xiàng運算yùnsuàn應該yīnggāi**很容易.**4** **舉Jǔ**一個例子: 我給你三千五百七十一和六千九百九十七. 你會乘以這些數字(我們都在學校學怎麼做了, 電腦甚**至**shènzhì比人類rén**lèi**做得更好), 一些步以後, 你知道這等於二四九八六二八七. 但另一方面, 如果我給你二四九八六二八七, 問你哪兩個數字可以**乘以**一起等於這個數字, 那你知不知道怎麼做呢? 如果我給你**其**中**qí**zhōng的一個數字, 那你會找到另外一個. 但是如果一個數字也不給你就很難找到它們.

Diànnǎo de chūxiàn dài láile xīn de mìmǎ xué fāngfǎ. Tāmen xīn de xiǎngfǎ rúxià: Zhǎodào yīgè shùxué **yùnsuàn** nǐ kěyǐ róngyì zuò, dànshì **diāndǎo** zhège **yùnsuàn** hěn nán. Nǐ xiǎng yào jiāmì de shíhòu, nǐ zuò zhège yùnsuàn. Nǐ xiǎng yào jiěmì de shíhòu, nǐ yào diāndǎo tā. **Dāngrán**, nǐ de péngyǒu kěnéng néng**gòu** **nì**zhuǎn zhège yùnsuàn. Rúguǒ tāmen zhīdào **mìmì**, **fǎn xiàng yùnsuàn** **yīng**gāi hěn róngyì. **Jǔ** yīgè lìzi: Wǒ gěi nǐ sānqiān wǔbǎi qīshíyī hè liùqiān jiǔbǎi jiǔshíqī. Nǐ huì chéng yǐ zhèxiē shùzì (wǒmen dōu zài xuéxiào xué zěnme zuòle, diànnǎo shènzhì bǐ rén**lèi** zuò dé gèng hǎo), yīxiē bù yǐhòu, nǐ zhīdào zhè děngyú èrsìjiǔbāliù'èrbāqī. Dàn lìng yī fāngmiàn, rúguǒ wǒ gěi nǐ èrsìjiǔbāliù'èrbāqī, wèn nǐ nǎ liǎng gè shùzì kěyǐ **chéng yǐ** yīqǐ děngyú zhège shùzì, nà nǐ zhī bù zhīdào zěnme zuò ne? Rúguǒ wǒ gěi nǐ **qí**zhōng de yīgè shùzì, nà nǐ huì zhǎodào lìngwài yīgè. Dànshì rúguǒ yīgè shùzì yě bù gěi nǐ jiù hěn nán zhǎodào tāmen.

Slide 33: Is the question posed at the end of the previous slide well-defined? Are there other pairs of integers which can be multiplied to get this number? A better question would be to ask if you can find all such pairs. It turns out that these questions are essentially equivalent. What we are trying to find is all divisors of a given integer. A prime number is an integer which is only divisible by itself and one. By successively dividing out by a prime number, we can break up a number into a product of many primes; this is known as the prime factorization. An encryption method known as RSA uses the fact that multiplication is easy but prime factorization is hard. Here’s an easier question to start with：can you even find all prime numbers?

在上一個**幻燈huàndēng**片最後的問題有**意義yìyì**嗎? 有可能有另外一對數字可以**乘chéng**以一起等於這個數字嗎? **1**更好的問題是: 你會不會找到所有的雙數字可以**乘以chéng yǐ**一起等於這個數字? 但是這些問題是**相**同**xiāng**tóng的.我們要找到的叫**除數chú shù** (在英文,我們說”divisors”). **2**一個**素數sù shù** (在英文說”prime number”)是一個**整數zhěngshù**, 它的**除數chú shù**只有自己跟一.**3** 如果你有一個整數,你可以找到一個**素數除數sù shù chú shù,** 然後你**除chú**以這個**素數除數sù shù chú shù,** 得到一個新的數. **重複Chóngfù**這個**過程guòchéng**給你這整數所謂的”prime factorization”. **4**一個叫”RSA” 的密碼系統的想法是乘法是容易但是”prime factorization”很難. **5**我們**從cóng**更容易的問題開始: 你能不能找到每個**素數**?

Zài shàng yīgè **huàndēng** piàn zuìhòu de wèntí yǒu**yìyì** ma? Yǒu kěnéng yǒu lìngwài yī duì shùzì kěyǐ **chéng** yǐ yīqǐ děngyú zhège shùzì ma? Gèng hǎo de wèntí shì: Nǐ huì bù huì zhǎodào suǒyǒu de shuāng shùzì kěyǐ **chéng yǐ** yīqǐ děngyú zhège shùzì. Dànshì zhèxiē wèntí shì **xiāng**tóng de. Wǒmen yào zhǎodào de jiào **chú shù** (zài yīngwén, wǒmen shuō”divisors”). Yīgè **sù shù** (zài yīngwén shuō”prime number”) shì yīgè **zhěngshù**, tā de **chú shù** zhǐyǒu zìjǐ gēn yī. Rúguǒ nǐ yǒu yīgè zhěngshù, nǐ kěyǐ zhǎodào yīgè **sù shù chú shù**, ránhòu nǐ **chú** yǐ zhège **sù shù chú shù**, dédào yīgè xīn de shù. **Chóngfù** zhège **guòchéng** gěi nǐ zhè zhěngshù suǒwèi de”prime factorization”. Yīgè jiào”RSA” de mìmǎ xìtǒng de xiǎngfǎ shì chéngfǎ shì róngyì dànshì”prime factorization” hěn nán. Wǒmen **cóng** gèng róngyì de wèntí kāishǐ: Nǐ néng bù néng zhǎodào měi gè **sù shù** ma?

Slide 34: Eratosthenes had an idea how to find every prime number up to a fixed bound. Since prime numbers are those numbers which are not divisible by any number but themselves, he would cross out all numbers that are multiples of another number. Here is an example where the primes up to 120. We start with 2 and cross out all even numbers. After that, the first number which is not crossed out is 3, and we see that it is prime. We cross out all multiples of three, and continue in this way until we’ve found all of the primes up to 120.

**1**“Eratosthenes” 有一個想法可以找到不**超**過**chāo**guò一個上**界jiè**的每個**素數sù shǔ**．因為他知道**素數sù shǔ**是沒有別的**除數chú shù**的整數，所以他**劃掉huà diào**有別的**除數chú shù**的整數，下一個還沒**劃掉huà diào**的數是**素數sù shǔ**．這裡有找到每個**素數sù shǔ**小於xiǎoyú一百二十的例子：**2**二是**素數sù shǔ**，所以每個雙數不是**素數sù shǔ**，然後三還沒**劃掉huà diào**，**因此yīncǐ**它是**素數sù shǔ**．因為九是三的**倍數bèishù**，所以它不是**素數sù shǔ**．十五也不是**素數sù shǔ**，等等．因為下一個還沒**劃掉huà diào**的整數是五，所以它是**素數sù shǔ**．我們**重複chóngfù**這個方法到一百一十三（它是最大的小於xiǎoyú一百二十的**素數sù shǔ**）．

“Eratosthenes” yǒu yīgè xiǎngfǎ kěyǐ zhǎodào bù **chāo**guò yīgè shàng **jiè** de měi gè **sù shǔ**. Yīnwèi tā zhīdào **sù shù** shì méiyǒu bié de **chú shǔ** de zhěngshù, suǒyǐ tā **huà diào** yǒu bié de chú shǔ de zhěngshù, xià yīgè hái méi huà diào de shù shì sù shù. Zhèlǐ yǒu zhǎodào měi gè sù shù xiǎoyú yībǎi èrshí de lìzi: Èr shì sù shù, suǒyǐ měi gè shuāng shǔ bùshì sù shù, ránhòu sān hái méi huà diào, **yīncǐ** tā shì sù shù. Yīnwèi jiǔshìsān de bèishù, suǒyǐ tā bùshì sù shù. Shíwǔ yě bùshì sù shù, děng děng. Yīnwèi xià yīgè hái méi huà diào de zhěngshù shì wǔ, suǒyǐ tā shì sù shù. Wǒmen **chóngfù** zhège fāngfǎ dào yībǎi yīshísān (tā shì zuìdà de **xiǎoyú** yībǎi èrshí de sù shù).

Slide 35: Now that we know it is possible to find all primes, let’s consider how to find the prime factorization of a number (that is to say, finding how to write it as a product of primes). Let’s consider the example of 144. We first note that it is even (i.e., it is a multiple of 2), and we divide by 2. We keep dividing by 2 until we get 9, and then we note that 9 is 3 times 3, so we get the prime factorization given here.

現在我們知道每個**素數sù shǔ**怎麼找到了．我們下一個問題是如果你有一個整數如何找到它的”prime factorization” (也就是說, 它是如何**表示biǎoshì**為**素數sù shǔ**的**乘積chéngjī**). **1**例如: 我們要找到一百四十四的”prime factorization”. **2**因為它是雙數shuāngshù, 我們用二**除chú**它.**3** 因為得到dédào的還是雙數, 所以我們還可以用二**除chú**它. **4**我們做了四次以後, 得到九. **5** 它就是三乘以三. 所以一百四十四等於二的四次**冪mì**乘以三的二次**冪**.

Xiànzài wǒmen zhīdào měi gè sù shù zěnme zhǎodàole. Wǒmen xià yīgè wèntí shì rúguǒ nǐ yǒu yīgè zhěngshù rúhé zhǎodào tā de”prime factorization” (yě jiùshì shuō, tā shì rúhé **biǎoshì** wèi sù shǔ de **chéngjī**). Lìrú: Wǒmen yào zhǎodào yībǎi sìshísì de”prime factorization”. Yīnwèi tā shì shuāngshù, wǒmen yòng èr **chú** tā. Yīn wéi dédào de háishì shuāngshù, suǒyǐ wǒmen hái kěyǐ yòng èr **chú** tā. Wǒmen zuò le sì cì yǐhòu, dédào jiǔ. Tā jiùshì sān chéng yǐ sān. Suǒyǐ yībǎi sìshísì děngyú èr de sì cì **mì** chéng yǐ sān de èrcì **mì**.

Slide 36: Let’s try to find the prime factorization of 481 now. It is odd, or in other words 2 does not divide iviede check that 3 does not divide it. Long division shows that 5, 7, and 11 do not divide it. We finally find that 13 divides it, and 481=13x37. Checking that 37 is prime, we see that this is precisely its prime factorization.

下一個例子: **1**我們想要四百八十一的**素數sù shǔ**分**解**fēn**jiě**, 找到它的”prime factorization”. **2**它是單數. **3** 三沒有分它.**4**五也沒有.**5**七也沒有.**6** 十一也沒有.**7** 十三分它! 四百八十一等於十三**乘以chéng yǐ**三十七. 因為三十七是**素數sù shǔ**所以這就是它的”prime factorization”.

Xià yīgè lìzi: Wǒmen xiǎng yào sìbǎi bāshíyī e sù shù fēn**jiě**, zhǎodào tā de”prime factorization”. Tā shì dānshù. Sān méiyǒu fèn tā. Wǔ yě méiyǒu. Qī yě méiyǒu. Shíyī yě méiyǒu. Shísān fēn tā! Sìbǎi bāshíyī děngyú shísān **chéng yǐ** sānshíqī. Yīnwèi sānshíqī shì sù shù suǒyǐ zhè jiùshì tā de”prime factorization”.

Slide 37: Let’s try to find the prime factorization of some larger numbers. Here’s an example. 2 doesn’t divide, 3 doesn’t divide, 5 doesn’t divide…. Ok, this could take a while… Finally we find that 1039 divides this number.

**1**現在, 我們試試用這個方法**處**理**chǔ**lǐ更大的整數. **2**這裡有一個例子. **3**二沒有分它, 三沒有分它, 五也沒有分它, 等等. 好了, 這個方法可能做很久…**4** 最後, 我們找到一個**除數chú shù**. **5**一千零三十九分它.**6** 請問: 十二萬七千五百四十九是**素數sù shǔ**嗎? 因為如果它有不同自己的**除數chú shù**, 一定有比它自己的**平方根píngfānggēn**更小的**除數chú shù**,所以它就是**素數sù shǔ**.

Xiànzài, wǒmen shì shìyòng zhège fāngfǎ **chǔ**lǐ gèng dà de zhěngshù. Zhèlǐ yǒu yīgè lìzi. Èr méiyǒu fèn tā, sān méiyǒu fèn tā, wǔ yě méiyǒu fèn tā, děng děng. Hǎole, zhège fāngfǎ kěnéng zuò hěnjiǔ…zuìhòu, wǒmen zhǎodào yīgè chú shù. Yīqiān líng sānshíjiǔ fēn tā. Qǐngwèn: Shí'èr wàn qīqiān wǔbǎi sìshíjiǔ shì sù shù, ma? Yīnwèi rúguǒ tā yǒu bùtóng zìjǐ de chú shù, yīdìng yǒu bǐ tā zìjǐ de píngfāng**gēn** gèng xiǎo de chú shù, suǒyǐ tā jiùshì sù shù.

Slide 38: We’re now going to see how this is used in cryptography. We saw in the previous slide that prime factorization is slow when the primes are large. RSA is a cryptographic system which uses this idea. (it is called RSA because Rivest, Shamir, and Adleman created it). How does RSA work? We start out by choosing two large prime numbers. We multiply the numbers together and send the answer to other people. This is freely-available (public) information, and we call this the “public key”. One needs the secret original primes to “unlock” the key (or do a long calculation); we call this secret information the “private key”.

現在, 我們要**討論tǎolùn**它在密碼學的用法. **1**在上一個**幻燈huàndēng**片, 我們看到**當dāng素數sù shǔ**因子yīnzǐ**變**biàn大的時候”prime factorization” 就**變**biàn慢了. RSA密碼系統就使用了這個想法 (因為Rivest, Shamir, 和Adleman**創造chuàngzào**了它, 所以我們叫它R-S-A). **2**RSA 是怎麼做呢? **3**開始的時候, 我們**選擇xuǎnzé**兩個很大的**素數sù shǔ**．然後，我們**將jiāng**這兩個數字**相xiàng**乘．**4把答案Bǎ dá'àn**發送給每個人．這就是公**共gòng**信息，就是所謂的公鑰匙．**5**想要用這個＂公鑰匙＂打開加密的信息的時候，你一定要知道**原始yuánshǐ**的兩個**素數sù shǔ**. **6**這兩個**素數sù shǔ**是秘密的信息, 就是” **私sī**鑰匙”. 你不知道它們的時候, 那你就**需xū**要做很長時間的計算.

Xiànzài, wǒmen yào **tǎolùn** tā zài mìmǎ xué de yòngfǎ. Zài shàng yīgè **huàndēng** piàn, wǒmen kàn dào **dāng** **sù shù** yīnzǐ biàn dà de shíhòu ”prime factorization” jiù biàn mànle. RSA mìmǎ xìtǒng jiù shǐyòngle zhège xiǎngfǎ (yīnwèi Rivest, Shamir, hé Adleman **chuàngzào**le tā, suǒyǐ wǒmen jiào tā R-S-A). RSA shì zěnme zuò ne? Kāishǐ de shíhòu, wǒmen **xuǎnzé** liǎng gè hěn dà de sù shù. Ránhòu, wǒmen **jiāng** zhè liǎng gè shùzì **xiàng** chéng. **Bǎ dá'àn** fasong gěi měi gèrén. Zhè jiùshì gōng**gòng** xìnxī, jiùshì suǒwèi de gōng yàoshi. Xiǎng yào yòng zhège"gōng yàoshi" dǎkāi jiāmì de xìnxī de shíhòu, nǐ yīdìng yào zhīdào yuánshǐ de liǎng gè sù shù. Zhè liǎng gè sù shù shì mìmì sī de xìnxī, jiùshì” **sī** yàoshi”. Nǐ bù zhīdào tāmen de shíhòu, nà nǐ jiù **xū**yào zuò hěn cháng shíjiān de jìsuàn.

Slide 39: Let’s get into some details. Suppose that Alice wants to send a message to Bob. First, she looks up Bob’s public key. The next step is to use this key to encrypt the information (this is similar to locking your front door). When the message arrives, Bob then uses his private key to “unlock” the message (i.e., decrypt the message). Although people in the middle can see the message, they cannot read the original message. The beauty of this encryption system is that Alice and Bob did not have to share any secret information beforehand! This is different than the other encryption methods that we have seen.

現在, 我們學一些RSA方法的**細節xìjié**. 第一個問題：公鑰匙／**私sī**鑰匙怎麼使用呢？**1**如果”Alice”想要給”Bob”發送消息, 她第一步是找到”Bob”的公鑰匙.**2** 下一步, 她使用”Bob”的公鑰匙加密消息**3** (這**類似lèisì**於**鎖**定**suǒ**dìng你公**寓**gōng**yù**的門). 加密的消息到”Bob”的時候，**4**他用他的**私sī**鑰匙解”**鎖suǒ”**這個消息(也就是說他**解密jiěmì**消息)．**5雖然Suīrán**在中間的人可以看到加密的消息，但是他們不能讀它．這個密碼系統最**驚**人**jīng**rén的事情shìqíng就是他們不用**提**前**tí**qián交**換**jiāo**huàn**秘密信息mìmì xìnxī．這跟我們學習xuéxí的另外一個密碼系統不同．因此Yīncǐ它比較bǐjiào好．

Xiànzài, wǒmen xué yīxiē RSA fāngfǎ de **xìjié.** Dì yīgè wèntí: Gōng yàoshi/**sī** yàoshi zěnme shǐyòngne? Rúguǒ”Alice” xiǎng yào gěi”Bob” fāsòng xiāoxī, tā dì yībù shì zhǎodào”Bob” de gōng yàoshi. Xià yī bù, tā shǐyòng”Bob” de gōng yàoshi jiāmì xiāoxī (zhè **lèisì** yú **suǒ**dìng nǐ gōng**yù** de mén). Jiāmì de xiāoxī dào”Bob” de shíhòu, tā yòng tā de**sī** yàoshi jiě” **suǒ**” zhège xiāoxī (yě jiùshì shuō tā **jiěmì** xiāoxī). Suīrán zài zhōngjiān de rén kěyǐ kàndào jiāmì de xiāoxī, dànshì tāmen bùnéng dú tā. Zhège mìmǎ xìtǒng zuì **jīng**rén de shìqíng jiùshì tāmen bùyòng **tí**qián jiāo**huàn** mìmì xìnxī. Zhè gēn wǒmen xuéxí de lìngwài yī gè mìmǎ xìtǒng bùtóng. Yīncǐ tā bǐjiào hǎo.

Slide 40: Let’s see a few more details about RSA. How does one specifically encrypt and decrypt the message in RSA? Firstly, you transform your message into numbers. The public key is a pair of integers ‘e’ and ‘N’.

那我們更**深**入**shēn**rù地看一下ＲＳＡ的**細節xìjié**．你怎麼加密？**1**你怎麼解密？**2**第一步：**將Jiāng**你的消息轉**化**zhuǎn**huà**為數字，這個數字我們叫’m’. **3**公鑰匙是一對整數’e’和’N’. **4**加密的消息xiāoxī是’m’ 的‘e’次**冪** **mì**(“modulo N”, **5**那個意思是我們用”modular arithmetic”). **6私Sī**鑰匙是那個’N’的**素數sù shǔ**分**解**fēn**jiě**和一個整數’d’. ‘d’ 的意思是‘m’的‘e’乘以’d’次**冪** **mì**“modulo N”就等於 ‘m’ 。

Nà wǒmen gēng **shēn**rù dì kàn yīxià RSA de **xìjié**. Nǐ zěnme jiāmì? Nǐ zěnme jiěmì? Dì yī bù**: Jiāng** nǐ de xiāo xí zhuǎn**huà** wéi shùzì, zhège shù zì wǒmen jiào’m’. Gōng yàoshi shì yī duì zhěngshù’e’ hé’N’. Jiāmì de xiāoxī shì’m’ de ‘e’ cì **mì** (“modulo N”, nàgè yìsi shì wǒmen yòng”modular arithmetic”). **Sī** yàoshi shì nàgè’N’ de sù shù fēn**jiě** hé yīgè zhěngshù’d’. ‘d’ de yìsi shì ‘m’ de‘e’ chéng yǐ’d’ cì **mì**“modulo N” jiù děngyú ‘m’ .

Slide 41: What are these numbers we used? ‘N’ is the product of two primes. The number ‘e’ is randomly chosen, and it is possible to compute ‘d’ once you know ‘e’ and the two prime numbers whose product is ‘N’. How do you compute it? The so-called “Chinese remainder theorem” tells you that you only need to find the answer modulo each prime divisor. Another theorem “Fermat’s little theorem” states that m to the power p is congruent to m modulo p for every prime p. If you have an encrypted message, how do you decrypt it? You raise it to the power d, since the encrypted message is m to the power e modulo N and m to the power d times e is equal to m modulo N.

**1**我們用的數字是甚麼？**2**’N’ 是兩個**素數sù shǔ**的乘**積**chéng**jī**．**3**那個數字’e’是**隨機選擇suíjī xuǎnzé**的．**4**如果你知道’e’和乘**積**chéng**jī**等於’N”的兩個**素數sù shǔ**的時候，你可以計算出那個’d’. 怎麼計算呢？所謂的”Chinese remiainder theorem” 說明’m’ 的‘a’次**冪mì**等於’m’ “modulo” ‘N’ **當且僅當dāng qiě jǐn dāng**’m’ 的‘a’次**冪mì**等於’m’ “modulo” N的每一個**素數sù shǔ**因子yīnzǐ．**5**所謂的”Fermat’s little theorem” 說明 如果’p’是**素數sù shǔ**，那’m’ 的‘p’次**冪mì**等於’m’ “modulo” ‘p’. **6**如果你有一個加密的消息，你怎麼**解密jiěmì**它呢？因為加密的消息等於’m’ 的‘e’次**冪mì** modulo N **而且érqiě** ’m’ 的‘e’乘以’d’次**冪**等於’m’ modulo N，所以**解密jiěmì**的方法是計算加密消息的‘d’次**冪mì** modulo N. **7**這個密碼系統的安全**性基於xìng jīyú**沒有乘**積**chéng**jī**等於’N”的兩個素數要計算’d’很难.

Wǒmen yòng de shùzì shì shénme?’N’ shì liǎng gè sù shǔ de chéng**jī**. Nà gèshùzì’e’ shì **suíjī xuǎnzé** de. Rúguǒ nǐ zhīdào’e’ hé chéng**jī** děngyú’N” de liǎng gè sù shǔ de shíhòu, nǐ keyi jìsuànchū nàgè’d’. Zěnme jìsuàn ne? Suǒwèi de”Chinese remiainder theorem” shuōmíng ‘m’ de ‘a’ cì**mì** děngyú’m’ “modulo” ‘N’ **dāng qiě jǐn dāng** ‘m’ de ‘a’ cìmì děngyú’m’ “modulo” N de měi yīgè sù shù yīnzǐ. Suǒwèi de”Fermat’s little theorem” shuōmíng rúguǒ’p’ shì sù shù, nà’m’ de ‘p’ cìmì děngyú’m’ “modulo” ‘p’. Rúguǒ nǐ yǒu yīgè jiāmì de xiāoxī, nǐ zěnme **jiěmì** tā ne? Yīnwèi jiāmì de xiāoxī děngyú’m’ de ‘e’ cìmì modulo N **érqiě** ’m’ de ‘e’ chéng yǐ’d’ cìmì děngyú’m’ modulo N, suǒyǐ jiěmì de fāngfǎ shì jìsuàn jiāmì xiāoxī de ‘d’ cìmì modulo N. Zhège mìmǎ xìtǒng de ānquán **xìng jīyú** méiyǒu chéng**jī** děngyú’N” de liǎng gè sù shǔ yào jìsuàn’d’hěn nán.

Slide 42: Here is an example of the RSA method. Let’s take the primes 17 and 13. Their product is 221. Fermat’s little theorem tells us that m to the power 16 equals one modulo 17 and m to the power 12 equals one modulo 13. An easy calculation implies that m to the power 48 is congruent to one modulo both 17 and 13, and the Chinese remainder theorem then tells us that m to the power 48 is congruent to one modulo 221.

**1**這是一個RSA方法的例子．我們**選擇xuǎnzé**的兩個**素數sù shǔ**是十七和十三．**2**他們的乘**積**chéng**jī**就是二百二十一． **3**“Fermat’s little theorem”說明’m’ 的十六次**冪mì**等於一modulo 十七**4**，’m’ 的十二次**冪mì**等於一modulo 十三**5**．我們很容易計算出’m’的四十八次**冪**cì**mì**等於一modulo 十七和它也等於一modulo 十三．**6**那個”Chinese Remainder Theorem” 說明它就等於一modulo二百二十一．

Zhè shì yīgè RSA fāngfǎ de lìzi. Wǒmen **xuǎnzé** de liǎng gè sù shù shì shíqī hé shísān. Tāmen de chéng**jī** jiùshì èrbǎi èrshíyī. “Fermat’s little theorem” shuōmíng’m’ de shíliù cìmì děngyú yī modulo shíqī,’m’ de shí'èr cì**mì** děngyú yī modulo shísān. Wǒmen hěn róngyì jìsuàn chū’m’ de sìshíbā cì**mì** děngyú yī modulo shíqī hé tā yě děngyú yī modulo shísān. Nàgè”Chinese Remainder Theorem” shuōmíng tā jiù děngyú yī modulo èrbǎi èrshíyī.

Slide 43: We next choose e=11. The number ‘d’ that we want to find should satisfy d times e equal to 1 modulo 48. However, this turns out to be equivalent to d times e congruent to 1 modulo 16 and also 1 modulo 3. Which ‘d’ satisfies the congruence “d times e congruent to 1 modulo 16”? Since 11 times 3 is 33, which is congruent to 1 modulo 16 (and there are not other solutions), we see that ‘d’ must be congruent to 11 modulo 16. Since ‘e’ is 2 modulo 3, ‘d’ must also be 2 modulo 3. Combining these, we obtain that ‘d’ is congruent to 35 modulo 48. Now let’s encrypt a message with this choice. Let’s say that the message is 12. We take 12 to the power 11 and find that this is 142 modulo 221. To decrypt this message, we take 142 to the power 35 and compute that this is 12 modulo 221.

**1**我們**選擇xuǎnzé**那個’e’等於十一．**2**我們想要找的’d’ **滿足mǎnzú**’e’乘以’d’等於一”modulo “四十八．因為’e’乘以’d’等於一”modulo”四十八,所以’e’乘以’d’就是一”modulo”十六也是一”modulo” 三. 哪一個’d’ **滿足mǎnzú**’e’乘以’d’等於一”modulo “十六呢? 因為三乘以十一等於三十三等於一”modulo “十六(也沒有其他qítā的**答案dá'àn**了), 所以’d’一定等於三”modulo”十六.**3** ‘e’ 等於二“modulo “三, 所以’d’也一定等於二”modulo” 三. **合Hé**在一起, 我們的**答案dá'àn**是’d’等於三十五”modulo” 四十八. 現在，**讓ràng**我們使用這個**選擇xuǎnzé**加密一**條tiáo**消息．**4**如果我們的消息就是十二，我們計算十二的十一次**冪**cì**mì**等於一百四十二”modulo “二百二十一．我們想要**解密jiěmì**的時候，我們計算一百四十二的三十五次**冪**cì**mì**等於十二”modulo “二百二十一．

Wǒmen **xuǎnzé** nàgè’e’ děngyú shíyī. Wǒmen xiǎng yào zhǎo de’d’ **mǎnzú** ’e’ chéng yǐ’d’ děngyú yī”modulo “sìshíbā. Yīnwèi’e’ chéng yǐ’d’ děngyú yī”modulo” sìshíbā, suǒyǐ’e’ chéng yǐ’d’ jiùshì yī”modulo” shíliù yěshì yī”modulo” sān. Nǎ yīgè’d’ **mǎnzú**’e’ chéng yǐ’d’ děngyú yī”modulo “shíliù ne? Yīnwèi sān chéng yǐ shíyī děngyú sānshísān děngyú yī”modulo “shíliù (yě méiyǒu qítā de dá'ànle), suǒyǐ’d’ yīdìng děngyú san ”modulo” shíliù. ‘e’ děngyú èr “modulo “sān, suǒyǐ’d’ yě yīdìng děngyú èr”modulo” sān. **Hé** zài yīqǐ yīqǐ, wǒmen de **dá'àn** shì’d’ děngyú sānshíwǔ”modulo” sìshíbā. Xiànzài, **ràng** wǒmen shǐyòng zhège **xuǎnzé** jiāmì yī**tiáo** xiāoxī. Rúguǒ wǒmen de xiāoxī jiùshì shí'èr, wǒmen jìsuàn shí'èr de shíyī cì**mì** děngyú yībǎi sìshí'èr”modulo “èrbǎi èrshíyī. Wǒmen xiǎng yào jiěmì de shíhòu, wǒmen jìsuàn yībǎi sìshí'èr de sānshíwǔcì **mì** děngyú shí'èr”modulo “èrbǎi èrshíyī.

Slide 44: There are other “one-way functions”. One example is “elliptic curve” cryptography. What is an elliptic curve, and what is the associated “one-way function”? These are (essentially) solutions to equations y squared equal to f(x), where f(x) is a polynomial of degree 3. Some points on this curve (that is to say solutions (x,y)) are (0,0), (1,0), (-1,0), (2,\sqrt{6}) (-2,\sqrt{6}), and so on.

還有**其**他**qí**tā一些”one-way functions”. **1**一個例子是所謂的”Elliptic Curve”密碼學系統．甚麼是這個”elliptic curve”呢？它的”one-way function”是什麼呢? **2**它就是每個對(x,y),它**滿足mǎnzú**y的二次**冪**cì**mì**等於f(x) . f(x) 是三次多**項**式duō**xiàng**shì. **3**例如”elliptic curve”: y的二次**冪**cì**mì**等於x的三次**冪**cì**mì減jiǎn** x. **4**我們找到一些在這個”elliptic curve”上的點(“點”的意思就是這個**等式的解**děng**shì de jiě**): (零,零), (一,零), (**負fù**一,零), (二, 六的平方**根**píngfāng**gēn**), (**負fù**二, 六的平方**根**) 就在這個”elliptic curve”上.

Hái yǒu **qí**tā yīxiē ”one-way functions”. Yīgè lìzi shì suǒwèi de”Elliptic Curve” mìmǎ xué xìtǒng. Shénme shì zhège”elliptic curve” ne? Tā de”one-way function” shì shénme ne? Tā jiùshì měi gè duì (x,y), tā **mǎnzú** y de èr cì **mì** děngyú f(x). F(x) shì sāncì duō**xiàng**shì. Lìrú”elliptic curve”: Y de èr cì**mì** děngyú x de sān cì**mì jiǎn** x. Wǒmen zhǎodào yīxiē zài zhège”elliptic curve” shàng de diǎn (“diǎn” de yìsi jiùshì zhège děng shì de jiě): (Líng, líng), (yī, líng), (**fù** yī, líng), (èr, liù de píngfāng**gēn**), (**fù** èr, liù de píngfāng**gēn**) jiù zài zhège”elliptic curve” shàng.

Slide 45: We can graph the solutions like this. Between any two points on the curve, there is a unique line. This line hits the curve in a unique third point. This third point comes from the fact that the polynomial has degree three.

**1**我們可以這樣**繪製huìzhì**這些”elliptic curve”上的點. **2通**過**Tōng**guò每兩個在”elliptic curve”上的點有一**條**yī**tiáo唯**一**wéiyī**的線xiàn. **3**在這**條tiáo**線上還有**唯**一**wéi**yī的另外第三個在”elliptic curve”上的點. 這第三個同时tóngshí在”elliptic curve”和線上的點的**存**在**cún**zài是因為這個多**項**式duō**xiàng**shì的次數是三.

Women kěyǐ zhèyàng **huìzhì** zhèxiē”elliptic curve” shàng de diǎn. **Tōng**guò měi liǎng gèzài”elliptic curve” shàng de diǎn yǒu yī**tiáo** **wéiyī** de xiàn. Zài zhè **tiáo** xiànshàng hái yǒu **wéi**yī lìngwài dì sān gè zài”elliptic curve” shàng de diǎn. Zhè dì sān gè tóngshí zài”elliptic curve” hé xiànshàng de diǎn de **cún**zài shì yīnwèi zhège duō**xiàng**shì de cìshù shì sān.

Slide 46: Elliptic curves have an “addition law”. This is called an “addition law” because it acts a lot like addition of integers. How does the addition work between two points on the elliptic curve? We find the third point lying on the line between these two points and the elliptic curve and then rotate around the x-axis. We also add a “point at infinity”

**1**“Elliptic curves” 有一個”addition law”. 它**被稱bèi chēng**為”addition law”是因為兩個點加法和兩個整數的加法很像. 如果你有兩個在”elliptic curve”上的點,那怎麼加他們呢? **2**我們找到第三個在**經過jīngguò**他們的線和”elliptic curve”上的點,**3** 然後**圍繞wéirào**”x-**軸zhóu**”旋轉. **4**我們也說在”elliptic curve”上有一個”點在無**窮qióng**”. **5**在”elliptic curve”上的無**窮qióng**點和整數的零很像. 為甚麼?

“Elliptic curves” yǒu yīgè”addition law”. Tā **bèi chēng** wèi”addition law” shì yīnwèi liǎng gè diǎn jiāfǎ hé liǎng gè zhěng shǔ de jiāfǎ hěn xiàng. Rúguǒ nǐ yǒu liǎng gè zài”elliptic curve” shàng de diǎn, nà zěnme jiā tāmen ne? Wǒmen zhǎodào dì sān gè zài **jīngguò** tāmen de xiàn hé”elliptic curve” shàng de diǎn, ránhòu **wéirào**”x-**zhóu**” xuánzhuǎn. Wǒmen yě shuō zài”elliptic curve” shàng yǒu yīgè” diǎn zài wú**qióng**”. Zài”elliptic curve” shàng de wú**qióng** diǎn hé zhěng shǔ de líng hěn xiàng. Wéishènme?

Slide 47: How does one add another point to infinity? For a point P, we choose the vertical line through P to be the “line between infinity and P”. If we write P=(x,y), then the other point this line is (-x,y). After rotating around the x-axis, we get (x,y), which is the point P. This helps us to understand why we say that infinity on the elliptic curve is like zero in the integers.

**1**“Elliptic curve”上的無**窮**wú**qióng**點和另外一個在”elliptic curve”上的點**相xiàng** 加呢? **2**如果你想要一個點P跟無**窮**wú**qióng**點**相xiàng**加, 我們說那**條經過tiáo jīngguò**點P的**垂chuí**線是**經過jīngguò**這兩個點的線.**3**如果P等於(x,y),在這個線也有(負x,y). **4圍繞Wéirào**”x-**軸zhóu**”旋轉到(x,y).**5**這就是那個點P. **6**現在, 我們**理解lǐjiě**為甚麼我們說無**窮**wú**qióng**點跟整數的零很像.

“Elliptic curve” shàng de wú**qióng** diǎn hé lìngwài yīgè zài”elliptic curve” shàng de diǎn **xiàng** jiā ne? Rúguǒ nǐ xiǎng yào yīgè diǎn P gēn wú**qióng** diǎn **xiàng** jiā, wǒmen shuō nà **tiáo jīngguò** diǎn P de **chuí**xiàn shì **jīngguò** zhè liǎng gè diǎn de xiàn. Rúguǒ P děngyú (x,y), zài zhège xiàn yěyǒu (fù x,y). **Wéirào**”x-**zhóu**” xuánzhuǎn dào (x,y). Zhè jiùshì nàgè diǎn P. Xiànzài, wǒmen **lǐjiě** wéishènme wǒmen shuō wúqióng diǎn gēn zhěng shǔ de líng hěn xiàng.

Slide 48: As an example for the addition law, let’s consider $y^2=x^3+x-1$. This elliptic curve has the points (1,1) and (2,3). The line y=2x-1 goes through these two points. By solving the equation defining the elliptic curve and the line simultaneously, we see that the third point on this line and the elliptic curve has x equal to 1.

**1**“Elliptic curve”加法的例子: **2**我們**選擇xuǎnzé** y的二次**冪**cì**mì**等於x的三次**冪**cì**mì**加x**減jiǎn**一定**義**dìng**yì**的”elliptic curve”. **3**點(一,一)和(二,三)在這個”elliptic curve”上. **4**這兩個點都在y等於二乘以chéng yǐ x**減jiǎn**一定**義**dìng**yì**的線上. 第三個在”elliptic curve”和線上的點一定**滿足mǎnzú**”elliptic curve” 定**義**dìng**yì**的方**程**fāng**chéng**和線定**義**dìng**yì**的方**程**fāng**chéng**. **5**我們**解jiě**這個方**程**fāng**chéng組zǔ**, 看到第三個點的x-坐**標**zuò**biāo**等於一.

“Elliptic curve” jiā fǎ de lìzi: Wǒmen **xuǎnzé** y de èr cì**mì** děngyú x de sān cì **mì** jiā x **jiǎn** yī dìng**yì** de”elliptic curve”. Diǎn (yī, yī) hé (èr, sān) zài zhège”elliptic curve” shàng. Zhè liǎng gè diǎn dōu zài y děngyú èr chéng yǐ x jiǎn yī dìngyì de xiàn shàng. Dì sān gè zài”elliptic curve” hé xiànshàng de diǎn yī dìng **mǎnzú**”elliptic curve” dìng**yì** de fāng**chéng** hé xiàn dìng**yì** de fāng**chéng**. Wǒmen **jiě** zhège fāng**chéng zǔ**, kàn dào dì sān gè diǎn de x-zuò**biāo** děngyú yī.

Slide 49: Altogether, we see that adding the points (1,1) and (2,3) on the elliptic curve yields the point (1,-1). Since the line connecting the points (1,1) and (1,-1) is a vertical line, we have (1,1) plus (1,-1) equal to the point at infinity (which we call zero on the elliptic curve). Since (1,1) plus (1,-1) equals zero on the elliptic curve, we call the point (1,-1) the negative of the point (1,1). Can one add a point to itself? If so, how does one do it? We’ve seen above that (1,1) plus (2,3) equals –(1,1) on the elliptic curve.

**1**一起, 我們現在看到, 在”elliptic curve”上的 點 (一,一) 加 點(二,三) 等於(一,**負fù**一). **2**因為對(一,一)和(一, **負fù**一)的線就是一**條垂tiáo chuí**線, 所以(一,一)加(一, **負fù**一)等於”elliptic curve”上的無**窮**wú**qióng**點(這是所謂的”elliptic curve addition law”的零). 因為(一,一)加(一, **負fù**一)等於”elliptic curve addition law”的零, **3**所以在”elliptic curve”上我們叫點(一, **負fù**一) **負fù**的點(一,一). **4**請問: 一個”elliptic curve”上的點可以和自己**相xiàng**加碼? 如果它可以, 那怎麼做呢?**5**在前面,我們看到在”elliptic curve”上的 (一,一) 加上 (二,三) 等於**負fù** (一,一), 所以**重**新chóngxīn安**排**ān**pái**意味**著**yìwèi**zhe** (一,一)加(一,一)等於**負**(二,三).

Yīqǐ, wǒmen xiànzài kàn dào, zài”elliptic curve” shàng de diǎn (yī, yī) jiādiǎn (èr, sān) děngyú (yī, fù yī). Yīnwèi duì (yī, yī) hé (yī, fù yī) de xiàn jiùshì yī**tiáo chuíxiàn**, suǒyǐ (yī, yī) jiā (yī, fù yī) děngyú”elliptic curve” shàng de wú**qióng** diǎn (zhè shì suǒwèi de”elliptic curve addition law” de líng). Yīnwèi (yī, yī) jiā (yī, fù yī) děngyú”elliptic curve addition law” de líng, suǒyǐ zài”elliptic curve” shàng wǒmen jiào diǎn (yī, fù yī) fù de diǎn (yī, yī). Qǐngwèn: Yīgè”elliptic curve” shàng de diǎn kěyǐ hé zìjǐ **xiàng** jiāmǎ? Rúguǒ tā kěyǐ, nà zěnme zuò ne? Zài qiánmiàn, wǒmen kàn dào zài”elliptic curve” shàng de (yī, yī) jiā shàng (èr, sān) děngyú fù (yī, yī), suǒyǐ **chóng**xīn ān**pái** yìwèi**zhe** (yī, yī) jiā (yī, yī) děngyú fù (èr, sān).

Slide 50: Does addition of a point with itself also have a geometric meaning? Is there a line that passes through the point twice? There isn’t, but if we choose another point really close to this point, then we can draw a line between these two points. If we keep picking closer and closer points, then we end up with a line that is called the “tangent line”.

**1**一個點和自己**相xiàng**加是**否**shì**fǒu具**有**jù**yǒu幾何jǐhé意義yìyì呢？**2**有**經過jīngguò**這個點兩次的線嗎？沒有，但是如果我們**選擇xuǎnzé**另外一個很近的點，然後我們可以畫huà一**條tiáo**線**經過jīngguò**這兩個點．**3**如果我們還在**選擇xuǎnzé**到這個點**越yuè**來**越yuè**近的點，那我們最**終zhōng**可以**獲huò**得那**條tiáo**所謂的”tangent line”．這**條tiáo**線**經過jīngguò**這個點，也與＂elliptic curve”相切．

Yīgè diǎn hé zìjǐ xiàng jiā shì**fǒu** **jù**yǒu jǐhé yìyì ne? Yǒu **jīngguò** zhège diǎn liǎng cì de xiàn ma? Méiyǒu, dànshì rúguǒ wǒmen **xuǎnzé** lìngwài yīgè hěn jìn de diǎn, ránhòu wǒmen kěyǐ huà yī **tiáo** xiàn **jīngguò** zhè liǎng gè diǎn. Rúguǒ wǒmen hái zài **xuǎnzé** dào zhège diǎn **yuè** lái **yuè** jìn de diǎn, nà women zuì**zhōng** kěyǐ **huò**dé nà **tiáo** suǒwèi de”tangent line”. Zhè **tiáo** xiàn **jīngguò** zhège diǎn, yě yǔ"elliptic curve” xiāng qiè.

Slide 51: What is three times the point (1,1) (by this, we mean the point added to itself 3 times). We have already computed that twice the point (1,1) equals the point (2,-3). Hence we want to add (1,1) to (2,-3).　A short calculation gives that the line going through these two points is y equal to -4x+5. Combining this equation with the equation for the elliptic curve yields that x=1,2, or 13. Since the other two points have x=1 and x=2, we conclude that x=13 for the third point. We can compute y=-47 from the equation for the line.

**1**三乘以chéngyǐ那點（一，一）等於甚麼（三乘以（一，一）的意思就是（一，一）給加本**身běnshēn**三次）？二乘以chéngyǐ（一，一）我們已經計算了．它等於（二，**負fù**三）. **2 因此Yīncǐ**我們想要計算了是（一，一）加（二，**負fù**三）．**3**一個小的計算**告訴gàosù**我們**經過jīngguò**這兩個點的線是y等於**負fù**四乘以chéngyǐ x加五．**4**這個方**程**fāng**chéng**跟”elliptic curve”的方**程**fāng**chéng**一起**決**定**jué**dìng了x等於一，二，還是十三．因為另外兩個點有x等於一和x等於二，所以第三個點一定是x等於十三的．我們使用線的方**程**fāng**chéng**找到y等於**負fù**四十七.

Sān chéng yǐ nà diǎn (yī, yī) děngyú shénme (sān chéng yǐ (yī, yī) de yìsi jiùshì (yī, yī) gěi jiā běn**shēn** sāncì)? Èr chéng yǐ (yī, yī) wǒmen yǐjīng jìsuànle. Tā děngyú (èr, fù sān). Yīncǐ wǒmen xiǎng yào jìsuànle shì (yī, yī) jiā (èr, fù sān). Yīgè xiǎo de jìsuàn **gàosù** wǒmen **jīngguò** zhè liǎng gè diǎn de xiàn shì y děngyú fù sì chéng yǐ x jiā wǔ. Zhège fāng**chéng** gēn”elliptic curve” de fāng**chéng** yīqǐ **jué**dìngle x děngyú yī, èr, háishì shísān. Yīnwèi lìngwài liǎng gè diǎn yǒu x děngyú yī hè x děngyú èr, suǒyǐ dì sān gè diǎn yīdìng shì x děngyú shísān de. Wǒmen shǐyòng xiàn de fāngc**héng** zhǎodào y děngyú fù sìshíqī.

Slide 52: Altogether, we get that three time (1,1) is (13,-47). If you want to compute 4 times (1,1), 5 times (1,1), and so forth, you can use the same method. The method is repetitive, so it is very easy to teach a computer how to compute n times a point on the elliptic curve (where n is a positive integer). Here’s a question: How fast, can you compute 100 times the point (1,1)?

**1**一起, 我們計算了三乘以(一,一)等於(十三, **負fù**四十七). **2** 如果你想要計算四乘以(一,一), 五乘以(一,一), 等等, **3**可以用一樣的方法. 因為這個方法是很**重複chóngfù**的, **4**所以很容易教一個電腦怎麼計算n乘以一個在”elliptic curve”上的點(那個n就是一個正整數zhèng zhěngshù). **5**請問:一百乘以(一,一),你可以多快計算了出來?

Yīqǐ, wǒmen jìsuànle sān chéng yǐ (yī, yī) děngyú (shísān, fù sìshíqī). Rúguǒ nǐ xiǎng yào jìsuàn sì chéng yǐ (yī, yī), wǔ chéng yǐ (yī, yī), děng děng, kěyǐ yòng yīyàng de fāngfǎ. Yīnwèi zhège fāngfǎ shì hěn **chóngfù** de, suǒyǐ hěn róngyì jiào yīgè diànnǎo zěnme jìsuàn n chéng yǐ yīgè zài”elliptic curve” shàng de diǎn (nàgè n jiùshì yīgè zhèng zhěngshù). Qǐngwèn: Yībǎi chéng yǐ (yī, yī), Nǐ kěyǐ duō kuài jìsuànle chūlái?

Slide 53: If you follow the method given before, you would have to add 100 times to compute 100 times a point. You can instead multiply by 2, then multiply that point by 2 to get 4 times the original point, then multiply that point by 2 to get 8 times the original point, and so on. Using this, 100 times the point is 64 times the point plus 32 times the point plus 4 times the point. We only need 8 sums to do this calculation! It is much less than 100!. In computer science, this type of trick is usually very helpful in speeding up computations.

**1**如果你用以前給的方法, 那你**需xū**要做這個加法一百次. 這個很慢. 但是加**倍bèi**在”elliptic curve”上的點也可以**重複chóngfù**做了. **2**加**倍****bèi**那個點兩次得到四乘以**原始yuánshǐ**的點. 加**倍bèi**四乘以**原始yuánshǐ**的點得到八乘以**原始yuánshǐ**的點,等等. **3**因為一百等於六十四加三十二加四,所以我們只要加**倍bèi**六次.**4** 一起,做八個加法就夠了.這個比以前學的方法更快! 一前的方法要**重複chóngfù**一百次,這個方法只**重複chóngfù**八次! 在計算**科kē**學中,這**種類似zhǒnglèi sì**的**訣竅juéqiào**可以加快計算**速度sùdù**很多.

Rúguǒ nǐ yòng yǐqián gěi de fāngfǎ, nà nǐ **xū**yào zuò zhège jiāfǎ yībǎi cì. Zhège hěn màn. Dànshì jiā**bèi** zài”elliptic curve” shàng de diǎn yě kěyǐ **chóngfù** zuòle. Jiā**bèi** nàgè diǎn liǎng cì dédào sì chéng yǐ **yuánshǐ** de diǎn. Jiā**bèi** sì chéng yǐ **yuánshǐ** de diǎn dédào bā chéng yǐ **yuánshǐ** de diǎn, děng děng. Yīn wéi yībǎi děngyú liùshísì jiā sānshí'èr jiā sì, suǒyǐ wǒmen zhǐyào jiā**bèi** liù cì. Yīqǐ, zuò bā gè jiāfǎ jiù. Zhège bǐ yǐqián xué de fāngfǎ gèng kuài! Yī qián de fāngfǎ yào **chóngfù** yībǎi cì, zhège fāngfǎ zhǐ **chóngfù** bā cì! Zài jìsuàn **kē**xué zhōng, zhè **zhǒnglèi sì** de **juéqiào** kěyǐ jiākuài jìsuàn **sùdù** hěnduō.

Slide 54: It helped to write 100 in a different way. What did we do to write it this way? We wrote its binary representation to get a faster algorithm. What is binary representation? Here ‘a’, ‘b’, ‘c’, and ‘d’ are all zero or one. Every positive integer has a unique binary representation. For example 1011 in binary equals 11.

在上個**幻燈huàndēng**片中，一百的另外一**種zhǒng**不同的分**拆chāi**幫了我們很多忙．我們怎麼寫它呢？**1**我們寫它所謂的二**進製表示jìn zhì biǎoshì**，得到了一個更快的運算**yùnsuàn**法則**fǎzé**（在英文二**進****製****表示jìn zhì biǎoshì**叫”binary representation”）．**進製表示jìn zhì biǎoshì**是甚麼？這裡的字母’a’,字母’b’,字母’c’,也字母’d’都是零還是一．每個正整數有**唯**一**wéi**yī的二**進製表示jìn zhì biǎoshì**．**3**例如：一零一一在二**進製表示jìn zhì biǎoshì**中等於十一．如果你想要二的n次**冪**cì**mì**乘以一個在”elliptic curve”上的點，你只**需**要**xū**yào一定用加倍jiā**bèi**ｎ次．**4**因為n比二的n次**冪**cì**mì**真的更小很多, **5**所以這個方法真的加快我們的計算了.

Zài shàng gè **huàndēng** piàn zhōng, yībǎi de lìngwài yīzhǒng zhǒng bùtóng de fēn chāi chāi bāngle wǒmen hěnduō máng. Wǒmen zěnme xiě tā ne? Wǒmen xiě tā suǒwèi de èr **jìn zhì biǎoshì**, dédàole yīgè gèng kuài de **yùnsuàn fǎzé** (zài yīngwén èr **jìn zhì biǎoshì** jiào”binary representation”). **Jìn zhì biǎoshì shì** shénme? Zhèlǐ de zìmǔ’a’, zìmǔ’b’, zìmǔ’c’, yě zìmǔ’d’ dōu shì líng háishì yī. Měi gè zhèng zhěngshù yǒu **wéi**yī de èr **jìn zhì biǎoshì**. Lìrú: Yī líng yīyī zài èr **jìn zhì biǎoshì** zhōng děngyú shíyī. Rúguǒ nǐ xiǎng yào èr de n cì **mì** chéng yǐ yi ge zài”elliptic curve” shàng de diǎn, nǐ zhǐ **xū**yào jiā**bèi** n cì. Yīnwèi n bǐ èr de n cì mì zhēn de gèng xiǎo hěnduō, suǒyǐ zhège fāngfǎ zhēn de jiākuài wǒmen de jìsuànle.

Slide 55: So what is the one-way function associated to elliptic curves? If I give you 1000 times a point on the elliptic curve, can you compute the original point? Above we saw that it is easy to compute 1000 times a point when given the point, but the reverse direction seems to be hard, and hence this is a “one-way function”. The public and private keys are usually smaller with elliptic curve cryptography, but it is harder to implement. This is often the cryptography usually used in Blockchain.

**1**那甚麼是”elliptic curve”使用的”one-way function”呢? **2**如果我給你一千乘以一個在”elliptic curve”上的點, 但是沒有給你這個**原始yuánshǐ**的點, 你可不可以計算這個**原始yuánshǐ**的點? 我們已經看到一千乘以一個在”elliptic curve”上的點怎麼計算了,但是**扭**轉**niǔ**zhuǎn這個計算人們覺得很難了,**3** 所以這個就是一個”one-way function”. **4** “elliptic curve”用的密碼**系統**有比ＲＳＡ更小**尺寸chǐcùn**的公鑰匙也**私**鑰匙sī yàoshi，所以這些鑰匙可以很快**創建chuàngjiàn**．它的問題是它在電腦上更難**實施shíshī**了．**5** ”elliptic curve”密碼**系統**是在**區塊qū kuài鏈liàn**上**經**常**jīng**cháng使用的密碼系統.

Nà shénme shì”elliptic curve” shǐyòng de”one-way function” ne? Rúguǒ wǒ gěi nǐ yīqiān chéng yǐ yīgè zài”elliptic curve” shàng de diǎn, dànshì méiyǒu gěi nǐ zhège **yuánshǐ** de diǎn, nǐ kěbù kěyǐ jìsuàn zhège **yuánshǐ** de diǎn? Wǒmen yǐjīng kàn dào yīqiān chéng yǐ yīgè zài”elliptic curve” shàng de diǎn zěnme jìsuànle, dànshì **niǔ**zhuǎn zhège jìsuàn rénmen juédé hěn nánle, suǒyǐ zhège jiù shì yīgè”one-way function”. “Elliptic curve” yòng de mìmǎ xìtǒng yǒu bǐ RSA gèng xiǎo **chǐcùn** de gōng yàoshi yě sī yàoshi, suǒyǐ zhèxiē yàoshi kěyǐ hěn kuài **chuàngjiàn**. Tā de wèntí shì tā zài diànnǎo shàng gèng nán **shíshī**le.”Elliptic curve” mìmǎ xìtǒng shì zài **qū kuài liàn** shàng **jīng**cháng shǐyòng de mìmǎ xìtǒng.

Slide 56: Is there a way to send a private key to share with someone else (these are usually called “session keys” because they are used together in shared sessions and both people can quickly encrypt and decrypt messages with the private key) without meeting that person beforehand to share the secret information? If I send you the private key, then someone else might steal it in between and replace it with their own; after this, they can pretend to be me. Here’s an idea: Maybe I can send you a private key encrypted with your public key (then it is locked so that only you can open it). How do you know that someone in between didn’t send you the private key, pretending to be me? You can send back a confirmation encrypted with my public key to verify that I’m really me. This is how “session keys” are sent.

**1**有沒有**辦**法**bàn**fǎ發送一個**私**鑰匙**sī** yàoshi與**其**他**qí**tā人一起使用（**2**這些通常tōngcháng**被稱bèi chēng**為”session keys”, 因為它們在**共享gòngxiǎng**會話huìhuà中一起使用得，兩個人都可以用私鑰匙更快地發送加密和**解**密消息），無**需**wú**xū**事先與**其**他**qí**tā人**共享gòngxiǎng** 秘密信息？ **3**如果我**向xiàng**你發送私鑰匙sī yàoshi，那麼在中間的**壞**人**huài**rén可能會**竊取qièqǔ**它，然後用它自己的私鑰匙; 以後，他們可以**假裝成jiǎzhuāng chéng**我． **5**一個想法：也**許**Yě**xǔ**我可以給你發一個用你的公鑰匙加密的**私**鑰匙**sī** yàoshi（然後它**被鎖住bèi suǒ zhù**了，**6**只有你可以打開它）． **7**你怎麼知道中間有人沒有給你發**私**鑰匙**sī** yàoshi，**假裝jiǎzhuāng**是我？ **8**您可以發回一份用我的公鑰匙加密的回**復**huí**fù**，校**驗**jiào **yàn**我真的是我．這是如何發送”session keys”.

Yǒu méiyǒu **bàn**fǎ fāsòng yīgè **sī** yàoshi yǔ **qí**tā rén yīqǐ shǐyòng (zhèxiē tōngcháng **bèi chēng** wèi”session keys”, yīnwèi tāmen zài **gòngxiǎng** huìhuà zhōng yīqǐ shǐyòng dé, liǎng gè rén dōu kěyǐ yòng sī yàoshi gèng kuài de fāsòng jiāmì han **jiě**mì xiāoxī), wú**xū** shìxiān yǔ **qí**tā rén **gòngxiǎng** mìmì xìnxī? Rúguǒ wǒ **xiàng** nǐ fāsòng sī yàoshi, nàme zài zhōngjiān de **huài**rén kěnéng huì **qièqǔ** tā, ránhòu yòng tā zìjǐ de sī yàoshi; yǐhòu, tāmen kěyǐ **jiǎzhuāng chéng** wǒ. Yīgè xiǎngfǎ: Yě**xǔ** wǒ kěyǐ gěi nǐ fā yīgè yòng nǐ de gōng yàoshi jiāmì de **sī** yàoshi (ránhòu tā **bèi suǒ zhù** shì guān**bì**le, zhǐyǒu nǐ kěyǐ dǎkāi tā). Nǐ zěnme zhīdào zhōngjiān yǒurén méiyǒu gěi nǐ fā **sī** yàoshi, **jiǎzhuāng** shì wǒ? Nín kěyǐ fā huí yī fèn yòng wǒ de gōng yàoshi jiāmì de huí**fù**, jiào **yàn** wǒ zhēn de shì wǒ. Zhè shì rúhé fāsòng”session keys”.

Slide 57: Let’s return to one of the difficult questions that we considered at the beginning.

我們回到我們開始的時候**考慮kǎolǜ**第一個問題．

Wǒmen huí dào wǒmen kāishǐ de shíhòu **kǎolǜ** dì yīgè wèntí.

Slide 58: Remember that we wanted to share a big calculation, but keep the data secret. Can you trust other people? If others use our encrypted data, can they still do the calculations that we want? If they can how can they do it?

**1**你記得，我們要**共享gòngxiǎng**一個很大的計算，但是還要**保密**數據. **2**你能**相xiāng**信別的人嗎？**3**如果別的人使用我們加密的消息，他們還可以做我們想要的計算嗎？**4**如果他們可以，那怎麼做呢？

Nǐ jìdé, wǒmen yào **gòngxiǎng** yīgè hěn dà de jìsuàn, dànshì hái yào **bǎomì** shù**jù**. Nǐ néng **xiāng**xìn bié de rén ma? Rúguǒ bié de rén shǐyòng wǒmen jiāmì de xiāoxī, tāmen hái kěyǐ zuò wǒmen xiǎng yào de jìsuàn ma? Rúguǒ tāmen kěyǐ, nà zěnme zuò ne?

Slide 59: For some data “m”, we write the encrypted message as E(m). We would like other people to add and multiply and get the correct answer when we decrypt the message after they do these operations. We would like to give people E(m) and E(n) and have them compute E(n) plus E(m) and E(n) times E(m). When we receive the answer, we should decrypt it and get either m plus n or m times n. Hence we would like to find a cryptosystem which satisfies the two equations below. Encryption which satisfies these two identities is known as “homomorphic encryption”.

**1**我們叫**原始yuánshǐ**的數據”m”. 如果我們使用一個密碼**系統**加密它，我們叫它E(m). **2** 我們想要的是給別的人E(m)和E(n), 然後他們可以計算E(m)加E(n) 和E(m)乘以E(n). **3**他們的**答案dá'àn**回來的時候，我們解密jiěmì它，解密jiěmì的數**據**shù**jù**就是m加n和ｍ乘以ｎ．所以，我們想要找到一個密碼系統，它**滿足mǎnzú**以下兩個等**式**děng **shì**.**4** 使用一個**滿足mǎnzú**以這兩個等**式**děng **shì**的密碼系統來加密就是所謂的”homomorphic encryption”.

Wǒmen jiào **yuánshǐ** de shùjù”m”. Rúguǒ wǒmen shǐyòng yīgè mìmǎ **xìtǒng** jiāmì tā, wǒmen jiào tā E(m). Wǒmen xiǎng yào de shì gěi bié de rén E(m) hé E(n), ránhòu tāmen kěyǐ jìsuàn E(m) jiā E(n) han E(m) chéng yǐ E(n). Tāmen de **dá'àn** huílái de shíhòu, wǒmen jiěmì tā, **jiě**mì de shùjù jiùshì m jiā n han m chéng yǐ n. Suǒyǐ, wǒmen xiǎng yào zhǎodào yīgè mìmǎ xìtǒng, tā **mǎnzú** yǐxià liǎng gè děng **shì.** Shǐyòng yīgè **mǎnzú** yǐ zhè liǎng gè děng **shì** de mìmǎ xìtǒng lái jiāmì jiu shì suǒwèi de”homomorphic encryption”.

Slide 60: Is “homomorphic encryption” possible? Have we seen any examples? Caesar cipher doesn’t satisfy either equality. RSA satisfies homomorphic multiplication, but not homomorphic addition.

**1**有可能做”homomorphic encryption”嗎？我們見過jiànguò這樣的例子嗎？**2**”Caesar cipher”不能做乘法和加法．**3**用RSA的時候，我們可以做"homomorphic"的乘法，但是不能做"homomorphic"的加法．

Yǒu kěnéng zuò”homomorphic encryption” ma? Wǒmen jiànguò zhèyàng de lìzi ma? ”Caesar cipher” bùnéng zuò chéngfǎ han jiāfǎ. Yòng RSA de shíhòu, wǒmen kěyǐ zuò"homomorphic"de chéngfǎ, dànshì bùnéng zuò"homomorphic"de jiāfǎ.

Slide 61: There are some rules for the encryption method of course. If someone in the middle sees a lot of encrypted data, they still shouldn’t be able to guess which one is zero and which one is one. There is a big problem, however: the rules given two slides ago imply that E(0)=0.

**1**一定有一些**規則guīzé**使得密碼系統是安全的**2**，如果在中間的**壞**人看到很多加密的消息，他們不能**猜測cāicè**哪一個是零和哪一個是一．**3**我們快看到一個大的問題：兩張**幻燈huàndēng**片上的等**式**děng **shì**意味**著**yìwèi**zhe** E(零)一定等於零．

Yīdìng yǒu yīxiē **guīzé:** shǐdé mìmǎ xìtǒng shì ānquán de, rúguǒ zài zhōngjiān de huàirén kàn dào hěnduō jiāmì de xiāoxī, tāmen bùnéng cāicè nǎ yīgè shì líng han nǎ yīgè shì yī. Wǒmen kuài kàn dào yīgè dà de wèntí: Liǎng zhāng huàndēng piàn shàng de děng shì yìwèizhe E(líng) yīdìng děngyúlíng.

Slide 62: Since 0 always gets encrypted to itself, you can always recognize it. Can we build a cryptosystem where homomorphic encryption is “mostly true”?

**1**因為加密的零就是零，所以人們可以認出rènchū它．**2**我們能不能**創建chuàngjiàn**一個密碼系統，它加密的數**據**大多**滿足****mǎnzú**”homomorphic encryption”的等**式**děng **shì**呢？**3**如果它只大多**滿足mǎnzú**這些等**式**děng **shì**，那你可不可以**相信xiāngxìn**它的**答案dá'àn**嗎？

Yīnwèi jiāmì de líng jiùshì líng, suǒyǐ rénmen kěyǐ rènchū tā. Wǒmen néng bùnéng **chuàngjiàn** yīgè mìmǎ xìtǒng, tā jiāmì de shùjù dàduō **mǎnzú**”homomorphic encryption” de děng **shì** ne? Rúguǒ tā zhǐ dàduō **mǎnzú** zhèxiē děng shì, nà nǐ kěbù kěyǐ **xiāngxìn** tā de **dá'àn** ma?

Slide 63: In 2009, Gentry found that one can add a little bit of “noise” to get “almost” homomorphic encryption. The noise is small compared to the answer, so it can be removed/cancelled later. Repeated calculations increase the noise, but it can be done many times before the noise gets too big to cancel it. This leads to homomorphic encryption, but it is quite slow.

**1**二零零九年，Gentry 發現可以**通過添**加**tōngguò****tiān**jiā一些”**噪**音**zào**yīn”, 差不多做得到 ”homomorphic encryption”. **2**這些**噪**音**zào**yīn比**答案dá'àn**更小很多，所以它還可以**稍**後**shāo** hòu**移除yí chú**（它**消除xiāochú**也可以說）．**重複Chóngfù**計算會增加**zēng**jiā**噪**音**zào**yīn**3**．**當****dāng噪**音**zào**yīn太大的時候，那我們不知道哪一個是**答案dá'àn**，哪一個是**噪**音**zào**yīn．用這個密碼**系統xìtǒng**，你會做很多計算, 沒有關**系**了méiyǒu guān**xì**le．你可以做很多計算，**4**然後回給**原版yuánbǎn**的人，所以他／她會**消除xiāochú噪**音**zào**yīn，那你在做很多計算了．用這個想法可以得到 ”homomorphic encryption”, **5**但是它還在很慢．

Èr líng líng jiǔ nián, Gentry fāxiàn kěyǐ **tōngguò** **tiān**jiā yīxiē” **zào**yīn”, chàbùduō zuò dédào”homomorphic encryption”. Zhèxiē **zào**yīn bǐ **dá'àn** gèng xiǎo hěnduō, suǒyǐ tā hái kěyǐ **shāo** hòu **yí chú** (tā **xiāochú** yě kěyǐ shuō). **Chóngfù** jìsuàn huì **zēng**jiā **zào**yīn. **Dāng zào**yīn tài dà de shíhòu, nà wǒmen bù zhīdào nǎ yīgè shì **dá'àn**, nǎ yīgè shì **zào**yīn. Yòng zhège **mìmǎ** **xìtǒng**, nǐ huì zuò hěnduō jìsuàn, méiyǒu guān**xì**le. Nǐ kěyǐ zuò hěnduō jìsuàn, ránhòu huí gěi **yuánbǎn** de rén, suǒyǐ tā/tā huì **xiāochú zào**yīn, nà nǐ zài zuò hěnduō jìsuànle. Yòng zhège xiǎngfǎ kěyǐ dédào”homomorphic encryption”, dànshì tā hái zài hěn màn.

Slide 64: The idea is based on the following observation: you can send something that you interpret as zero but other people don’t. For example, both midnight and noon are zero on a clock. If you didn’t know how many hours a clock had, though, then you wouldn't know that 0, 12, and 24 were all the same thing. So you send the data in one way, but interpret it differently yourself. This is the basis of Gentry’s idea.

這個想法使用以下開始點：**1**你可以發送別人你**解釋jiěshì**為等於零的數據，**2**但是如果他們用他們用自己的**解釋jiěshì**，那他們不知道它等於零．**3**例如：午**夜**Wǔ**yè**和中午在時鐘上都是零點，**4**但是如果別的人類不知道你的時鐘有十二個小時，**5**那他們也不知道零，十二，和二十四都是一樣時間了．**6** 所以我們發送數據給人一個**表示biǎoshì**, **7**但是我們自己對數據的解釋是不同的．這就是Gentry想法的**基礎jīchǔ**．

Zhège xiǎngfǎ shǐyòng yǐxià kāishǐ diǎn: Nǐ kěyǐ fāsòng biérén nǐ **jiěshì** wèi děngyúlíng de shùjù, dànshì rúguǒ tāmen yòng tāmen yòng zìjǐ de **jiěshì,** nà tāmen bù zhīdào tā děngyúlíng. Lìrú: Wǔ**yè** hé zhōngwǔ zài shízhōng shàng doū shì língdiǎn, dànshì rúguǒ bié de rénlèi bù zhīdào nǐ de shízhōng yǒu shí'èr gè xiǎoshí, nà tāmen yě bù zhīdào líng, shí'èr, hé èrshísì dōu shì yīyàng shíjiānle. Suǒyǐ wǒmen fāsòng shùjù jǐ rén yīgè **biǎoshì**, dànshì wǒmen zìjǐ duì shùjù de jiěshì shì bùtóng de. Zhè jiùshì Gentry xiǎngfǎ de **jīchǔ**.

Slide 65: There are now LOTS of zeros, so we can pick a different way to write zero each time we send a message. Someone would have to figure out that these are all zero to recognize it. Of course, this pattern is too simple (like “Caesar Cipher”), so people in the middle can recognize it.

**1**所以我們現在有好多好多的零數．每次我們有新的我們想要加密的信息，我們**選擇xuǎn zhái**不同的零．如果別人想要看得**懂**kàn dé **dǒng**我們加密的消息，他們一定**認識rènshí**這些不同的零真zhēn的都是零．**2**因為這個**模式móshì**太**簡**單了**jiǎn**dānle（和”Caesar cipher”的難**度**nán**dù**差不多一樣），所以別的人可以**猜測cāicè**哪一個是零．

Suǒyǐ wǒmen xiànzài yǒu hǎoduō hǎoduō de líng shù. Měi cì wǒmen yǒu xīn de wǒmen xiǎng yào jiāmì de xìnxī, wǒmen **xuǎn zhái** bu tóng de líng. Rúguǒ biérén xiǎng yào kàn dé dǒng wǒmen jiāmì de xiāoxī, tāmen yīdìng **rènshí** zhèxiē bùtóng de líng zhēn de dōu shì líng. Yīnwèi zhège **móshì** tài **jiǎn**dānle (han”Caesar cipher” de nán**dù** chā bù duō yīyàng), suǒyǐ bié de rén kěyǐ **cāicè** nǎ yīgè shì líng.

Slide 66: We hence need to combine this trick with some other ideas. We have to also do something to the data so that it isn’t clear that it is 0, 12, 24, etc. (but the changed cryptosystem still needs to satisfy the identities of homomorphic encryption). Most methods either don’t appear to be safe or they are too slow to do any practical calculations.

**1因此Yīncǐ**我們需用**結合jiéhé**這個想法跟別的想法．**2**我們要**改變gǎibiàn**這個數據，使得別人不知道它是零，十二，二十四，等等（但是這個**改變gǎibiàn**數據的密碼系統**仍然réngrán**需要**滿足mǎnzú**”homomorphic encryption”的等**式**děng **shì**！）．**3**大部分bùfèn方法不安全就是做**實際shíjì**計算太慢了.

**Yīncǐ** wǒmen xūyào **jiéhé** zhège xiǎngfǎ gēn bié de xiǎngfǎ. Wǒmen yào **gǎibiàn** zhège shùjù, shǐdé biérén bù zhīdào tā shì líng, shí'èr, èrshísì, děng děng (dànshì zhège **gǎibiàn** shùjù de mìmǎ xìtǒng **réngrán** xūyào mǎnzú”homomorphic encryption” de děng **shì**!). Dà bùfèn fāngfǎ bù ānquán jiùshì zuò shíjì jìsuàn tài mànle.

Slide 67: It’s time to get back to work and find the answer! Thank you very much for coming to the talk. I hope that you enjoyed it. Are there any questions?

那我們要回去工作，和**尋**找**xún**zhǎo答案了．謝謝大家來聽過我的**演講yǎnjiǎng.** 我**希望xīwàng**你們喜歡它．你們還有問題嗎？
Nà wǒmen yào huíqù gōngzuò, hé **xún**zhǎo dá'ànle. Xièxiè dàjiā lái tīngguò wǒ de **yǎnjiǎng.** Wǒ **xīwàng** nǐmen xǐhuān tā. Nǐmen hái yǒu wèntí ma?