ИВАН ЗЛАТАРСКИ
БЕЛЕЖКИ ПО РОМАНА „ЦИФРОВА КРЕПОСТ“, ИЗД. „БАРД“, 2004

(Тези бележки — с една дребна фактологична промяна — бяха създадени по време на работата над превода, но включването им бе отказано, както ми бе съобщено, по настояване на агента, представляващ автора в България.)

Когато преди две години отворих за първи път тази книга с молба от издателството да дам евентуална препоръка за превод, първото ми впечатление беше леко тревожно. Проблемът бе, че книгата безспорно се четеше, но в нея изобилстваха редица твърдения от технически и технологичен характер, които обхващаха деликатния за коментиране спектър от лекото преиначаване до откровената неистина. Обяснението за някои от тях е желанието да се подходи „по-творчески“ и да се огънат някои факти в удобна за сюжетните линии посока (примерно така мисля, че стоят нещата с „квадрата на Цезар“), при други става дума за недостатъчно познаване на темата (доста неща от кухнята на криптографията) и най-сетне в трети видях съзнателно изопачаване („Скипджак“ и най-общо заставането на позиция, от която АНС се вижда само в сянка и в ролята на „лошия“). Докато работих над превода започнах да мисля, че това не само не бива да бъде препятствие, а напротив — възможност да се разкаже истината, такава каквато е, още повече, че понякога фактите са не по-малко интересни от фикцията. Малкото, което се знае за криптографията (наука на повече от две хилядолетия) и крайно ограниченият брой романи, в които тя играе основна роля, ми дадоха основание да се опитам да разкажа малко повече, та макар и само за неща, имащи отношение към сюжета. Вече бях прочел „Пътеводителя към Шифъра на Леонардо“ и за да не се ограничавам с кратки бележки под линия, реших да постъпя точно по обратния начин: възможно *най-подробно* да изясня другата (истинската) страна на нещата в исторически правилния контекст. Ползвах различни източници, но най-вече читателските отзиви в „Амазон“ (бих оценил съотношението чужди-мои на 70:30). Анонимността на повечето от тях ме лишава от възможността да изкажа благодарността си към понякога изумителната наблюдателност на някои от критиците. Преднамерено избрах само онези, които засягат едни или други технически аспекти, и съзнателно съм филтрирал всички нападки към подробности на сюжета, образите на героите и особеностите в тяхното поведение и мотивировка — за тях смятам, че

авторът е в правото си да има пълна свобода. Старал съм се да се въздържам от ирония или сарказъм, но ако тук-там понякога пробива елемент на насмешливост, това е само в няколко единични случаи на действително забавни грешки. За което искрено се извинявам.

И така…

Има два начина да се чете тази книга: единият е да й се наслаждавате такава каквато е, другият е да оставите неточностите в нея да ви отровят удоволствието. А има и трета възможност: да научите истината. Пътеводителят по-долу има за цел да помогне на любопитния читател.

• **„Огромни букви известяваха КРИПТО“** (гл.3) — авторът благодари на анонимни бивши служители на АНС, на които дължал част от получената информация. В случая обаче по-правдоподобно изглежда написаното от най-известния изследовател на АНС Джеймс Бамфорд (автор на единствените две книги за тази организация), според който в Крипто Сити надписите на офисите са максимално неинформативни за непосветения, напр. 2W106 — някога директорския офис, или 2B8020 — голямата заседателна зала и т.н. Във всеки случай, крайно невероятно е движещ се по подземен тунел човек (това не може да бъде случаен посетител) да се изправи пред врата като на хранилище, на която с едри букви да пише услужливо какво се намира от другата й страна. Дори ако забравим за маниакалната за АНС секретност, безсмислеността на подобен акт е очевидна.

• **„варианти на раницата“** (гл.3) — става дума за т.н. *knapsack* алгоритъм (предложен от Ралф Меркъл в средата на 70-те години), имащ отношение към криптографията с публично известен ключ, считан за кратко за алтернатива на т.н. RSA-алгоритъм. Меркъл неколкократно предлагал награди за този, който разбие схемата му (и дори ги плащал!), докато накрая му омръзнало и признал, че този алгоритъм просто не става за криптографски цели. Не е ясно защо авторът споменава това понятие в конкретния контекст.

• **„те бяха част от писмото, известно като канджи“** (гл.3) — тук вероятно има някакво недоразумение: Бекър опитва да декодира на „мандарин“, после казва на криптоаналитиците, че всички символи, които вече е превел, са също и част от „канджи“ (японска система за писане) и че на „канджи“ тези китайски символи имат различно

значение. Първо, това не се нарича „канджи“; второ, използваните в японския език „канджи“ (което означава „китайски символи“) имат еднакъв смисъл на японски и китайски. С други думи, фрагмент на „канджи“ (да използваме това понятие) ще бъде лишен от японската граматика, но ще се чете без никакъв проблем (примерно като група от глаголи и съществителни).

• **„шифърът на Цезар, използващ точен квадрат“** (гл.3) — описваният шифър не е на Цезар и не е известен под това име. Всъщност, поради неговата пределна елементарност, той дори няма име и не е известно кой пръв го е предложил или използвал. Може най-общо да се каже, че е от транспозиционен тип (разместване на буквите на открития текст в шифрограма), от който има т.н. шифри с „колонна транспозиция“ (вписване на текста по редове в правоъгълник и снемане по колони, но в ред, определен от ключова дума, т.е. разбъркано). Историята познава *шифър на Цезар*, но той е съвсем друг и е от субституционен тип (заместване на буквите). Знае се, че Цезар е изпращал шифровани писма, в които всяка буква се заместувала с отстоящата на три позиции след нея, т.е. D вместо A, E вместо B, F вместо C и т.н. Толкова голямо било значението на тази схема за времето си, че всички шифри, при които шифровата азбука е отместена на фиксирано разстояние спрямо основната, започнали да се наричат „цезарови азбуки“. Неясно защо авторът изневерява на историческата истина и макар малко по-късно в рамките на същата глава да дава пример за истински „цезаров шифър“, той не уточнява това.

• **„Разчитането му било възможно само от онзи, който притежавал същата машина, настроена по същия начин както шифроващата“** (гл.3 — става дума за шифъра на „Енигма“) — Изказаното твърдение не е вярно. Още преди войната полски математици намерили начин да разчитат шифрограми, създадени с „Енигма“ (вярно, не толкова заради криптографски слабости на машината, колкото заради пропуски в процедурата по използването ѝ). По-късно те предали опита си на англичаните, които в продължение на цялата Втора световна война успешно разчитали шифрограмите на Вермахта (т.н. „Операция Ултра“).

• **„Плексигласовото покритие бе с вложена с него фина мрежа от поликарбонат и осигуряваната по този начин защита можеше да устои на взрив с мощност два мегатона“** (гл.4) — това е някакво

недоразумение, понеже никакъв земен материал не може да устои на звездните температури, развивани в епицентъра на атомен взрив. Милионите градуси просто биха превърнали в плазма всичко не само в епицентъра, но и в непосредствена близост.

• **„Прозрачната материя филтрираше слънчевата светлина“** (гл.4) — АНС е разположила най-секретния си компютър под купол с прозрачно (та макар и не напълно) покритие? Това просто е невъзможно.

• **„Това бе TRANSLTR“** (гл.4) — авторът естествено е в правото си да използва всякакво име за хипотетичен компютър. Но (а) какъв смисъл е бил търсен в половинчатото съкращение (от translator/translate), и (б) как си представя авторът, че го наричат криптоаналитиците (неговите, тези в романа) помежду си (човешкият език някак се връзва при произнасянето на 8-буквена дума с единствена гласна в нея).

• **за криптографията с публичен ключ** (гл.4) — авторът я описва некоректно като възникнала в резултат на нуждата от тайни комуникации (в частност при имейлите). Но това е най-общото обяснение за нуждата от криптографията по принцип. Идеята е по-друга: в средата на 70-те години Уолтър Дифи и Мартин Хелман публикуват основополагаща статия, в която излагат принципно нова концепция, при която всеки участник в схемата разполага с два ключа: таен (личен) и публично известен (и лесно достъпен от всеки). Тази схема носи две предимства: (а) няма нужда от дистрибуция на ключовете (основен недостатък и голямо затруднение при класическите системи от симетричен тип) — нужно е само достъпно за всички място, където надеждно да се съхраняват публичните ключове, и (б) възможност за идентификация на изпращача. Ето как става това на практика: изпращачът кодира (използва алгоритъма на правата трансформация) откритият текст с публично известния ключ на получателя, който след това го декодира (прилага алгоритъма на обратната трансформация) със своя таен ключ (само онзи, който знае тайния ключ, може да декодира успешно съобщения, кодирани с публичния). Това осигурява секретността. Когато иска да „подпише“ изпратеното съобщение, изпращачът го кодира втори път със своя личен ключ. Сега получателят първо декодира съобщението с публичния ключ на подателя и после действа както преди. Ако се

получи читаем текст, значи шифрограмата е била изпратена наистина от човека, комуто е известен трайния ключ (всичко на практика е доста по-сложно, но това най-общо е принципът и той много успешно се използва вече четвърт век).

• **„Да се познае ключа при това положение бе толкова безнадеждно, колкото да се избере правилната песъчинка от петкилометров плаж“** (гл.4 — става дума за ключ, позволяващ 10^{120} пермутации) — използваното сравнение е толкова слабо, че дори не започва да дава представа за големината на число от този порядък. Като пример, според някои физически теории броят на протоните в наблюдаемата от нас Вселена е от порядъка на 10^{80}, т.е. число много по-малко от посоченото. Броят на песъчинките в „петкилометров“ плаж е нищожно малко число в сравнение с кое да е от двете по-горе. Съвсем произволна сметка показва, че ако една песъчинка тежи 0.001 грама, а пясъкът на петкилометровия плаж тежи примерно 1 милиард тона (т.е. 10^{15} грама — определено завишена оценка) то в него има от порядъка на примерно 10^{18}–10^{20} песъчинки. Дори тази елементарна сметка показва, че става дума за коренно различен порядък на размера на числата (изразяващи броя на комбинациите) в съвременната криптография.

• **„Пет години, половин милион човеко-часа и 1.9 милиарда долара по-късно“** (гл.4) — авторът явно се опитва да ни впечатли. И наистина, инвестиция от 2 милиарда долара! Само че какво показват сметките: половин милион човекочаса за 5 години означават по 100000 на година, което при 2000 работни часа на човек за година (50 седмици по 40 работни часа), означава, че суперкомпютърът е бил построен от някакви 50-ина души, което не само не е смайващо начинание, а по-скоро граничи с невъзможен за изпълнение подвиг.

• **„Последният…микропроцесор бе запоен ръчно… и керамичният корпус бе заварен“** (гл.4) — ненужни подробности, които само задълбочават липсата на достоверност. Ръчно (защо?) запояване на 3 милиона процесора за половин милион човекочаса означава по 6 процесора на час, т.е. по един на десет минути, което извиква в съзнанието нелепата картина на 50 човека трескаво запояващи на 10 минути по процесор, осем часа на ден в продължение на пет години; при това положение невъзможността да се заварява керамика (заварява се само метал) изглежда като дребен пропуск.

• **„…заместник-директора по оперативните въпроси, командър Тревор Дж. Стратмор…“** (гл.4) — след като директорът на АНС е по правило генерал с четири звезди, изключено е неговият заместник да има чин/ранг „командър“, това е еквивалентно на „капитан 3-и ранг“ — унизително нисък чин за висш служител на АНС, комуто (както разбираме по-нататък) на всичко отгоре предстои да се пенсионира (т.е. би следвало вече да е израсъл в йерархията).

• **„Бученето на генераторите идваше…“** (гл.5) — тези генератори ще бучат през цялата книга, но това би имало смисъл само, когато токът спре. За какво иначе ще работят генератори? Всъщност АНС е вторият по големина консуматор в щата и използва автономно захранване само в екстрени ситуации (колкото и невероятно да изглежда при всички грижи за непрекъсваемост на работата, на 24 януари 2000 година всички компютърни системи на АНС претърпяват тотален срив — случаят е описан във втората книга на Джеймс Бамфорд за АНС — Body of Secrets).

• **„необичайно дълъг ключ… десет хиляди бита“** (гл.5) — авторът (вж. и по-нататък) смята, че шифър се разбива по метода на грубата сила (т.е. с пълно изчерпване на комбинациите) като се анализира една малка част от него, примерно 64-бита, после се преминава на следващата група от 64-бита и т.н. Това, разбира се, изобщо не е вярно — нищо не може да подскаже на човек или компютър, че даден фрагмент от ключа е открит и може да се анализира следващия. Малко по-нататък Сюзан споменава, че TRANSLTR разбива 64-битов ключ за 10 минути. Но понеже добавянето на един бит удвоява числото (с един бит се представят две числа „0“ и „1“, с два — четири: „00“, „01“, „10“ и „11“ и т.н.), тогава 65-битов ключ ще се разбива за 20 минути, 66-битов — за 40 минути и т.н. В тази връзка 10000-битов ключ е непосилно дълъг за всеки компютър (сегашен или бъдещ) от класически неквантов тип (ако изобщо приемем, че квантовият компютър е възможен). Откриването на правилната комбинация при такава дължина по метода на грубата сила предполага брой операции и времена на обработка, за която човешкият разум няма опорни понятия (най-общо може да се каже, че ако Вселената ни само ще се разширява, нужно е време, несравнимо по-дълго от това, за което цялата материя във Вселената ще се изпари в

лъчение). **„Един час“** — колкото се е мъчил TRANSLTR — показва тотално неразбиране на сложността на проблема.

• **„сегментиран ключ с дължина един милион бита“** (гл.3 — обработен за 3 часа) — това вече е просто нелепо (вж. предния коментар).

• **„Става дума за неразбиваем шифър“** (гл.5, гл.29 и на още много места) — неразбиваем алгоритъм/шифър — тази книга бе широко дискутирана в Интернет (както споменах, част от тези бележки са заимствани от анонимни читатели, дали своите отзиви за различни твърдения от технически и технологичен характер, споменавани в нея) и много критици правилно посочват, че т.н. „неразбиваем шифър“ в никакъв случай не може да се смята за нова и едва ли не едва ли не революционна идея в криптографията, понеже още през 1917 година Джозеф Моборг и Гилбърт Върнам предлагат т.н. „шифър за еднократна употреба“ (*one-time pad* или OTP). Идеята им е пределно проста: всяка буква на изходния (открит) текст да се шифрова с една *случайно* генерирана буква на ключа. В първоначалната си форма шифроването ставало, като се използвало събиране по модул 26 (в английски език има 26 букви и всяка буква може да се кодира с поредния ѝ номер в азбуката: „0“ за A, „1“ за B … „25“ за Z). По-конкретно буквите се кодират с техните поредни номера в азбуката, започвайки от 0 (за „A“) и стигайки до 25 (за „Z“). Нека предположим, че искаме да кодираме **CIPHER** (02–08–15–07–04–17) с напълно случайния набор от символи (за ключа) **UTEQFD** (20–19–04–16–05–03). Събирането на всяко число, отговарящо на буква от изходния текст, със съответно число, отговарящо на буква от ключа, дава: 22–27–19–23–09–20, което (имайки предвид, че 27 mod 26 = 01, остатъкът от деленето на 27 на 26) декодирано в букви дава шифровия текст **WBTXIU** (по-късно операцията „събиране по модул“ била сменена с логическа операция от рода „изключващо ИЛИ“ — известна като „сума по модул 2“ — и др., но това не променя принципа). Теоретично не съществува метод за разбиване на подобен шифър, защото случайната природа на ключа разрушава всякаква изходна структура в откритията текст, а търсенето на такава е в основата на криптоанализа. Без да се знае ключът, е безпредметно да се опитва дешифриране, защото друг ключ би дал друг изходен текст, например изпробването на ключ **UKVIQG** върху все същия шифров текст **WBTXIU** би дало

напълно възможната дума от откритият текст **CRYPTO** и по същия начин извъртането на всички възможни ключове би върнало всички възможни изходни комбинации, без критерий за избор на правилната). При това положение Сюзан наистина не би следвало да се удивлява на съществуването на „неразбиваем шифър“, понеже като „главен криптолог“ на АНС тя би трябвало най-добре да знае, че такъв има и то отдавна. Нещата щяха да бъдат наистина прости, ако Дан Браун използваше в книгата си само термина „неразбиваем шифър“. За съжаление той използва (без да се придържа към утвърдените дефиниции за тези тях) още и „неразбиваем код“ и „неразбиваем алгоритъм“. *Неразбиваем код* действително не съществува, понеже кодовете (термин, използван от автора в неправилен контекст) представляват шифри със заместване като могат да се заместват както букви, така и цели думи. Работата е в това, че за кодиране се използват „кодови книги“, а това предполага тяхното многократно използване, което вече означава наличието на достатъчно количество прехванат шифров материал за статистическа обработка (както и използване на ред специфични за криптоанализ на кодовете методи). По-сложен е въпросът със съществуването на *неразбиваеми алгоритми* — на него е трудно да се отговори еднозначно и криптографията се въздържа да даде окончателен отговор. Съвременните блокови шифри със симетричен ключ по правило са от т.н. Файстелов тип: блокът се разбива на две половини, върху всяка от тях се използва нелинейна операция с т.н. S-кутии, при които група битове се замества от таблица с друга група с различен размер, после върху двете половини се прилага криптографска функция със индивидуален за дадената итерация ключ, след това двете половини разменят местата си и това се повтаря толкова пъти — итерации — колкото предвижда алгоритъмът на шифъра. Файстел-шифрите се атакуват с общи методи от рода на линейния или диференциален криптоанализ, но не е изключено за всеки отделен шифър да бъдат разработени специфични методи (използващи особености/слабости на реализираната криптографска функция). Но дори за даден шифър (от алгоритмичен тип) да се установи, че е устойчив на *досега* известните ни методи за криптоанализ, няма никакъв начин да се предскаже, че той ще бъде устойчив и срещу всички *бъдещи* методи. Така че въпросът за

съществуването на „неразбиваем алгоритъм“ е много далеч от окончателен отговор (и такъв може би по принцип не може да се даде).

• **„принципът на Бергофски“** (гл.5 и гл.31) — в историята на криптографията няма нито такова лице, нито има такова твърдение.

• **„Пи-Джи-Пи, Дифи-Хелман, ЗИП, ИДЕА, Ел Гамал“** (гл.5) — става дума за PGP (това не е шифър или криптографски алгоритъм, а система/програма за зашифроване на имейл), Diffie-Hellman (протокол за обмен на ключове), ZIP (алгоритъм и програма за компресиране на файлове), IDEA (единственият шифроващ алгоритъм сред изброените) и El Gamal (алгоритъм в състава на групата за криптосистеми с публично известен ключ).

• **„Идеята за функция осъществяваща цикличен открит текст бе изложена за пръв път в малко известна статия от 1987 година на унгарския математик Йожеф Харни“** (гл.5) — никакво търсене в Интернет не откри нито „rotating clear text“, нито „Josef Harne“ (независимо дали криптолог или математик). Остава да се предположи, че както „принципът на Бергофски“, „сейфът на Бигълман“ (вж. по-нататък) и др., това е измислица на автора, но самата идея да се шифрова даден текст така, че той магически да се самомодифицира при изпробване на различни ключове, за да не може компютърът да „познае“, че е намерил правилния ключ, е като идеята за барон Мюнхаузен, дето се измъкнал от блатото, дърпайки се за косата.

• **„Зашифровал е «Цифрова крепост» с самия себе си“** (гл.7) — това твърдение е в стил „параграф–22“ и ето защо: притежаването само на ключа не позволява да се разкодира програмата, трябва да е налице и самата програма, която шифрова/дешифрира с даден ключ. С други думи, на сайта на Танкадо трябва да има веднъж кодираната програма и второ програмата, с която тя е кодирана. Проблемът е, че ако Танкадо публикува изпълнимата програма, възможен е т.н. *reverse engineering* процес (най-общо казано дисасемблиране на изпълнимия код), за да се разбере алгоритъмът на работата й — АНС биха могли да направят това (с техните възможности) за секунди и тогава вече няма да им е необходим и изходният код (написан на някакъв програмен език) на самия алгоритъм, който е бил зашифрован. От друга страна, ако е предложен (както излиза от описанието в книгата) само кодираният програмен файл, тогава той е неизползваем с или без

ключа. Горе-долу същото съображение е в основата и на твърдението, че само с ключ, без да се знае алгоритъма, използван с този ключ, не е възможно да се разшифрова нищо нито по метода на грубата сила, нито с който да е друг, защото компютърът няма да знае какви обратни операции (дешифриране с пробен ключ) да прилага, ако в него не е въведена информация за правите (зашифроване с ключа).

• **„сейфът на Бигълман“** (гл.7) — няма такова лице, нито в криптографията съществува такова понятие.

• **„Като предпазна мярка всеки подаван на TRANSLTR файл първо се обработваше от «Гонтлит» — навързани последователно шлюзове, пакетни филтри и дезинфекциращи програми, които сканираха входящите файлове за компютърни вируси и потенциално опасни фрагменти от код в тях. Файловете, съдържащи непознат за «Гонтлит» програмен код, биваха безкомпромисно отхвърляни и се отделяха за ръчна проверка“** (гл.8) — този дълъг фрагмент изважда някои логически противоречия, състоящи се в следното: „Гонтлит“ предварително анализира файловете, които TRANSLTR впоследствие ще разшифрова, като търси „потенциално опасни фрагменти“ в тях. Само че как ще стане това, след като на тази програма се подава кодиран файл, чието съдържание (ако шифърът изобщо си струва да се подава на TRANSLTR) е близко до случайно по характер. Т.е. „Гонтлит“ не може предварително да анализира файловете, защото TRANSLTR още не е разбил дадения шифър. От друга страна, ако на „Гонтлит“ се подава текст на програма (не изпълним файл, а преди компилацията), тогава за TRANSLTR не остава нищо да се прави.

• **„бактериални вируси“** (края на гл.9) — взаимно изключващи се понятия. Бактерия е общо наименование на жив микроорганизъм, *притежаващ клетъчна структура*, докато вирусът е ултрамикроскопичен *неклетъчен* организъм, своеобразен вътреклетъчен паразит, размножаващ се само в живите клетки.

• **„анонимен сървър“** (гл.10) — обяснението на автора, че имейлът се изпраща до псевдоним, който анонимният имейл-сървър превръща в реален адрес и го изпраща на желания получател, е неточно. Всъщност, вярно е *обратното*: анонимният имейл-сървър е инструмент за запазване анонимността на *подателя*. Обменът на информация по Интернет (в това число изпращането на имейли) става

чрез използване на различни протоколи от протоколния стек TCP/IP. Най-общо казано информацията се разбива на пакети с нужния размер и всеки пакет (освен другата служебна информация) съдържа две полета с т.н. IP-адреси (комбинация от четири/шест еднобайтови числа) на подателя и на получателя. Ролята на анонимния сървър (независимо дали е имейл- или прокси-сървър) е да подмени IP-адреса на *подателя* със своя (или в някои случаи дори да го остави празен). Фактът на подмяната би могъл (но не е задължително) да се регистрира със запис в журнален файл (и следователно в изключителни случаи да бъде възможно обратното трасиране на имейла). Независимо от случая, в *получения пакет* няма никаква информация, позволяваща да се идентифицира оригиналния *подател* — верижката прекъсва при анонимния сървър, такава е същността на идеята. Това, което авторът предлага, е безсмислено, понеже за откриване на имейл акаунт (кутия за електронна поща) не е необходимо да се предоставя истинска информация: yahoo.com, hotmail.com, hushmail.com, email.com, gmail.com и още десетки (ако не стотици) доставчици на Интернет-услуги от много години насам с готовност предлагат безплатна електронна поща (т.н. *уеб-базирана*, т.е. необвързана с конкретен Интернет-доставчик, електронна поща), а за получаването на имейл адрес е достатъчно да се попълни (онлайн) формуляр с какво да е име, псевдоним и парола.

• **Трейсърите** (гл.10) — според автора може да се прикачи програма към невинно изглеждащ имейл и тя да изпрати до подателя си истинския адрес на получателя на така манипулираната електронна поща. Макар това по принцип да е възможно (в крайна сметка съвременните вируси се разпространяват чрез заразени имейли и те наистина могат да изпълняват ред опасни операции на компютъра), (а) не е задължително получената поща да се отваря (което би активирало трейсъра), а може направо да се изтрие, както би постъпил всеки благоразумен човек, получил поща от неизвестен подател, (б) дори да се отвори заразената поща, ако „дупките“ на операционната система са били редовно „закърпвани“ (*patched*), изпълнението на така програма няма да е възможно, то ще бъде блокирано с или без известяващо съобщение, и най-сетне (в) използването на персонални защитни стени (firewall-програми от рода на Internet Connection Firewall в състава на Windows XP, OutPost Pro, Norton Personal Firewall, ZoneAlarm и още

десетки безплатни и скъпоструващи такива) ще информира потребителя, че нещо (някаква програма) се опитва да се свърже с Интернет (за да изпрати обратно IP-адреса му) и дори да разреши това, той ще бъде предупреден, че „има нещо не наред“. С две думи, ако „трейсърът“ на Сюзан бе възможен, досега Интернет да беше удавен от вируси (поради възможността прикачен към имейл изпълним файл да разбере, че е стигнал до адреса си, и да се самостартира по някакъв магически начин).

• **„Стратмор бе гениален криптолог-програмист, но репертоарът му се свеждаше основно до разписване на алгоритми“** (гл.10) — „разписването на алгоритми“ е възможно най-ниското стъпало в кариерата на един програмист. Ако Стратмор наистина е такъв, това не се връзва с думата „гениален“, а по-скоро с констатацията „безнадеждно задръстен“.

• **Езикът „Лимбо“** (гл.10) — създаден от Денис Ричи (създател и на езика C), Лимбо е програмен език за използване в операционната система Инферно (за създаване и поддържане на разпределени услуги), т.е. той е предназначен за писане на приложения, свързани с реализирането на разпределени системи на малки компютри. Синтаксисът му, който естествено е различен, в значителна степен е подобен на този на езика C (който пък е може би най-разпространеният от всички програмни езици). Макар по принцип това да би било възможно, средствата на Лимбо в никакъв случай не са най-подходящите за реализиране на онзи вид специфично Интернет-програмиране, което един „трейсър“ предполага. Що се отнася до термина „хибриден“ (в смисъл „производен на няколко, смес от няколко“) той не е приложим към Лимбо (дотолкова, доколкото той само наподобява донякъде C и нищо друго).

• **„Екипът *(на АНС — бел. пр.)* сигурно щеше да вярва, че операцията има нещо общо с наркотиците“** (гл.10) — АНС няма нищо общо с борбата срещу разпространението на наркотиците и никакви нейни отряди не могат да изпълняват подобни задачи (нахлуване в частен дом); всичко свързано с наркотиците, е работа или на ФБР или на Бюрото за борба с наркотиците (DEA — Drug Enforcement Administration, агенция към американското Министерство на правосъдието — имаща еднаква юрисдикция с тази на ФБР по отношение борбата с наркотиците на американска почва).

• **64 бита и 64 символа** (гл.16) — авторът бърка двете: вътрешното (в паметта на компютъра) кодиране на цифра/буква/специален знак става с помощта на т. н. ASCII-таблица (по времето, когато е писан романа, 1996 година, още не се е използвало т.н. UNICODE-кодиране, при което, за да се обхванат основните световни азбуки, се използва дори 16-битово/2-байтово кодиране). Така че с низ от 64-бита могат да се кодират 8-символа, които не са чак толкова трудни за запомняне. По-късно разбираме, че въпросният ключ е 26-символен, т.е. не става дума нито за 64-бита, нито за 64-символа.

• **„Златото е вечно“** (гл.16). — Образно казано, това може и да е вярно, но практически погледнато, точно златото е много мек метал и лесно се износва, така че гравиран върху него надпис би имал ограничено време на живот.

• **„Скипджак“** (гл.23) — блоков шифър (размер на блока 64 бита, 80-битов ключ, 32-итерации), разработен от АНС през 1985–1990 г., предназначен за вграждане в предизвикалите (в САЩ) голяма полемика крипто-чипове Clipper и Capstone, поради което АНС запазила алгоритъма му в тайна (не защото това подобрявало сигурността му, а защото не е искала той да бъде използван по друг начин, освен като хардуерна реализация в споменатите чипове, т.е. не са искали той да се разпространява из целия свят като програма). Така че към 1996 година (когато е написана тази книга) АНС все още *не била* публикувала алгоритъма (както твърди авторът), точно напротив — *най-ревниво е пазела тайната му*. След провала на двата чипа (Clipper — заради лошата реализация на идеята за отделен, известен на трета страна ключ, Capstone — заради неудачите с компютърната крипто-карта Fortezza, в която бил използван), през 1999 (след публикуването на „Цифрова крепост“) АНС взема решение да разсекрети алгоритъма на „Скипджак“, и оттогава той вече може да се използва и под формата на софтуер (проектиран е с оглед удобство при вграждане в 8-битови контролери и има минимални изисквания към оперативната памет). Последвалият обстоен анализ на алгоритъма (това е единственото вярно твърдение на автора по отношение на „Скипджак“), в това число от корифеи на криптологията с безукорна репутация (напр. Рон Ривест) бил особено интересен, защото за първи път АНС правела публично достояние свой продукт (при това така дълго разработван). Никакви „задни врати“ все още не са открити в

него, напротив, общоприетото мнение е, че е много умно и икономично конструиран. По днешните стандарти обаче се смята за относително бавен (заради 32-те си итерации), а 80-битовата дължина на ключа се приема за недостатъчна, за да гарантира достатъчна надеждност в средносрочен план (в наши дни се използват блокови шифри със 128–, 192- и дори 256-битови ключове, както е да кажем във вече одобрения за национален стандарт (**AES**) шифър Rijndael). Големият проблем на „Скипджак“ било точно дългото му пазене в тайна (1990–1999), през което време се появили не по-малко бързи, поне толкова икономични и още по-надеждни шифри — той просто бил остарял.

• **„Вместо монитор имаше течнокристален индикатор, монтиран в лявото стъкло на чифт очила…. сега потребителят можеше да гледа *през* своите данни и да продължава активно да взаимодейства с околния свят“** (гл.25) — в интерес на истината, течнокристалните индикатори са непрозрачни, т.е описваната технология не може да бъде реализирана на такъв тип компоненти.

• **„С няколко бързи движения тя извика програма на име «СкрийнЛок»«** (гл.29) — вярно, че книгата е писана през 1995–6, но дори и в онова време вече отдавна имаше скрийнсейвъри, защитени с парола и опитът на автора да ни представи този възможно най-елементарен и общодостъпен продукт като ново средство, предоставено на разположение на криптолози (и други държавни служители), за да си пазят информацията и то не къде да е, а точно в АНС… този опит — меко казано — е връх на наивността

• **»задна врата“** (back door) (гл.31) — „дупка“ в защитата/ сигурността на система (шифър или операционна система на компютър), оставена от създателите й. Зад наличието на такива дупки не винаги се крие злоумисъл. Понякога става дума за небрежно програмиране, друг път — за привилегирован достъп, оставен например за облекчаване на инсталацията. Практиката познава много случаи на „задни врати“: прословутият „червей“ на Робърт Морис от 1988 използва „задна врата“ в програмата „sendmail“ на ОС BSD Unix; през 1983 Кен Томпсън (създател на Unix) разкрива в лекцията си по повод получаване на наградата „Тюринг“, че в ранните версии на Unix е имало една от най-коварните „задни врати“ в цялата история на компютрите — в С-компилатора (с който се е компилирала както

цялата операционна система, така и нейни отделни модули) е имало код, който е разпознавал прекомпилирането на командата login и е вмъквал в нея код, позволяващ на Томпсън да влиза със специална парола във всяка Unix-система, дори без да е притежавал акаунт в нея. Коварството на Томпсън било в това, че компилаторът е разпознавал случаите, когато компилирал сам себе си (компилатора) и в този случай вмъквал в кода си допълнителен код, който впоследствие ставал част от login-командата… както и код, позволяващ да разпознава бъдещата си собствена компилация, разбира се. Конкретно в историята на криптографията може би най-известен е случаят с дискусиите около приемането на шифъра DES. За съжаление, мястото тук не позволява случилото се да бъде разказано с всички съпътстващи го пикантни подробности (те могат да бъдат намерени във великолепната книга на Стивън Леви „Крипто“ (1991)). Впрочем, ето накратко за какво става дума… През 1973 и после 1974 година, NBS (National Bureau of Standards, днес NIST) публикува изискванията за публични предложения за нов шифър, който да бъде приет като национален стандарт. По онова време в IBM работи знаменитият Хорст Файстел (швейцарски евреин), който упорито и с успех разработва шифъра „Луцифер“ (първоначално известен като „Демон“ — от „демонстрация“). През 1973 година Файстел публикува принципите, на които според него трябва да бъдат изградени солидните блокови шифри (вж. бележката за „неразбиваемите шифри“ по-горе). Всички те са залегнали в „Луцифер“, който е блоков шифър със 128-битов ключ и 16 итерации. Една от големите новости, приложени от Файстел в него са т.н. „S-боксове“ („S“ от substitution или „заместване“). Те представляват нелинеен елемент в шифъра и за онова време са абсолютна новост. Бели петна в биографията на Файстел след емигрирането му в САЩ карат някои изследователи да подозират, че всъщност идеята е била подхвърлена на Файстел не от кой да е друг, а от служители на АНС (които официално нямат право да изнасят под никаква форма информация, свързана с вътрешните разработки на Агенцията). Целта била да се създаде максимално солиден шифър. Екип на IBM под ръководството на Уолт Тъчман (в началото с участието и на Файстел, който обаче малко по-късно е накаран да напусне IBM), разработва предложение за национален шифър, чието име първоначално е DSD, а после DES (от **D**ata **E**ncryption **S**tandard).

Всъщност… други предложения нямало — това било зората на компютърните шифри. Макар АНС да била сериозно обезпокоена от солидността на единственото предложение, времето било такова, че се изключвала възможността от „удобна“ публична намеса — това са годините след скандала Уотъргейт, години на сериозни съмнения в почтеността на институциите. Както и да е, DES също е 16-рундов, но използва два пъти по-къс ключ — „само“ 64-битов. След консултации между Тъчман и АНС дори тази дължина (въпреки несъгласието на Файстел) била намалена на 56-бита с оправданието, че „загубените“ 8 бита са за контрол по четност на съдържанието на останалите 8 байта (1 байт = 8 бита). Според Тъчман само така IBM би могла да произведе интегрален вариант на DES (по тогавашната 2-микронна C-MOS технология). Днес няма съмнения, че АНС е натиснала IBM да облекчи работата ѝ, съкращавайки ефективната дължина на ключа. По-мистериозна е ситуацията около S-боксовете. Ето накратко каква е същността им: всеки S-бокс (при DES) е таблица от четири реда и 16 колони, в клетките на която са записани числа в интервала 0–15 (понеже числата са 4 пъти по-малко от клетките на таблицата, ясно е че в нея има повторения на елементите). DES използва 8 различни S-бокса. Една от операциите по време на всяка итерация е заместването на 6-битови блокове от текущо преобразувания текст (6 бита дават възможност за точно 64 комбинации) с 4-битови елементи от някой от S-боксовете (спецификацията на DES дефинира какво се прави във всеки момент). Излишно е да се споменава, че съдържанието на S-боксовете не е случайно, нещо повече, именно те придавали на DES силата му. Само че екипът на Тъчман не стига до крайния им вариант веднага. Знае се за поне една станала публично известна промяна. Най-подозрителното било, че хората от IBM отказали да разкрият принципите, към които са се придържали, за да стигнат до конкретното съдържание на всеки от осемте S-бокса. Както и да е, DES бил одобрен, приет и веднага взет на въоръжение от десетки милиони потребители. Десетилетия наред банките поверявали на него сигурността и тайната на транзакциите си. Но съмненията, че Тъчман е заложил в DES чрез дадените му от АНС (и може би удобни за Агенцията) S-боксове скрита „задна врата“ (в онези времена техническият термин бил *trap door*) продължили да витаят из публичното пространство. Дискусиите не спирали, но никой не се

изправил да даде доказателства за нечиста игра. Мистерията започнала да се разплита едва в началото на 90-те години. Тогава двама млади евреи публикували нов вид криптоанализ, който нарекли „диференциален“ и който разработили специално за атака срещу файстеловите шифри (резултатите им могат да се намерят в *Differential Cryptanalysis of the DES* by Eli Biham, Adi Shamir, 1993). Най-любопитното в заключението им било, че те могли да се справят с най-различни облекчени варианти на DES (по-малко на брой итерации, различен ред на прилагане на S-боксовете, различно съдържание на S-боксовете). Буквално *всеки друг* вариант бил уязвим по един или друг начин. Но пълният вариант в оригиналния му вид бил удивително устойчив на този вид криптоанализ: най-добрият им резултат бил метод за атака, при който вместо 2^{56} изпробвания на различни ключове, колкото предполага методът на грубата сила (brute force), стигали „само“ 2^{47} двойки шифрован-открит текст с избран открит текст (този резултат бил леко подобрен впоследствие от Мацуи, автор на „линейния криптоанализ“ — 2^{43} двойки с известен открит текст). Изглеждало сякаш Тъчман и хората му били големи късметлии да изберат точно 16 на брой итерации и да се спрат точно на тези S-боксове (които спъвали успеха на диференциалния криптоанализ). Няколко години по-късно от IBM официално разкрили, че изобщо не ставало дума за късмет. Дон Копърсмит (един от участниците в създаването на DES) публикувал мистериозните критерии (7 на брой) при проектирането на S-боксовете и допълнително се разбрало, че 20 години преди Бихам и Шамир, Тъчман и хората му използвали т.нар. „T-атака“, която по същество представлявала диференциален криптоанализ. И именно T-атаката била обект на големия (и тогава изглеждащ доста подозрителен) интерес на АНС, където естествено отдавна знаели и използвали тази атака (под друго, вътрешно за АНС, име). Всъщност най-голямото признание за „чистотата“ на DES идва много години по-късно: един ден Алан Конхайм (участник в екипа на Уолт Тъчман) разговарял неофициално с Хауърд Розенблум — заместник-директор на АНС по развойната дейност. Извън протокола Розенблум „подхвърлил“ (само че служители на АНС това ниво никога не се „изпускат“ случайно) по повод DES: „Вие тогава се справихте *прекалено* добре“. За Конхайм това било най-голямото признание за труда им. Този разговор трябва да се е провел след 1998, когато

споменаваната в този роман ФЕГ построила специализиран компютър (състоящ се от 1536 чипа, работещи на 40MHz тактова честота) на стойност $200 000 (2/3 от които за материали), с чиято помощ DES бил официално разбит за средно 4.5 денонощия на едно търсене на ключ. По оценки на ФЕГ, с по-голям бюджет (не 1500, а примерно 300 000 чипа) най-добрият възможен резултат на избраното от тях хардуерно решение би бил около половин час. Според участниците в този проект, всяка по-голяма и уважаваща себе си страна в света разполага с DES-кракър. Само за сведение ще спомена, че още през 60-те години в АНС пресмятали компютърната си база не на бройка, а… на декари площ. При това става дума не за обикновени, а за супер-компютри. Тази сбито разказана дълга история показва, че не винаги АНС е големият злодей, макар срещу Агенцията наистина да могат да се отправят множество основателни упреци. А „задната врата“ конкретно в „Скипджак“, както вече споменах, изобщо е измислица.

• **„бъг“** (гл.34) — подобна история е разказана от адмирал Грейс Хопър (една от създателките на езика „Кобол“, автор на идеята за компилатор, останала запомнена с много остроумни фрази, сред които например „По-лесно е да получиш прошка, отколкото да издействаш разрешение“). Към нея следва да се направи уточнението, че става дума за „Марк II Aiken Relay Computer“, (а не „Марк 1“), а (това вече наистина само за любителите на големите подробности) релето е било #70, на платка F. Освен това, случилото се е не през 1944, а точно на 9.9.1945. След като компютърът е бил „Марк II“, а не „Марк 1“, той не може да е бил първият — за *първи цифров електронен* компютър се смята този на Атанасов-Бери, създаден през 1937–1942 в Университета на Айова (в него са използвани логически вериги, двоична аритметика и регенеративна памет). Макар да признава, че не е присъствала на случилото се, адмирал Хопър въвела в употреба термина „бъг“ като шеговито обяснение на причината за неизправна работа на компютър. Нещо повече, в продължение на дълги години дневникът с описанието на начина на отстраняване на повредата и прикрепеният към страницата конкретен молец били изложени във витрина в Naval Surface Warfare Center (а самата история е изложена съвсем официално в *Annals of the History of Computing*, Vol. 3, No. 3 (July 1981), pp. 285–286). В наши дни терминът се използва най-вече за програмни грешки.

• **„… понякога имаше и *външни* причини: резки промени в захранващото напрежение, частици прах по печатните платки на компютъра, проблеми с окабеляването“** (гл.34) — личи си, че авторът няма техническо образование. Възможните резки промени в захранващото напрежение (дори да допуснем, че такива могат да се появят не къде да е, а точно в АНС, където всичко е многократно дублирано с непрекъсваеми източници на захранване) могат да спрат работата на компютъра, а не на *програмата*; същото се отнася и до прашинките по платките — евентуалното „късо“ от прашинка между две шини на платка ще спре компютъра с операционната му система и всички изпълнявани в този момент десетки други (макар и само системни) програми, а не единствено трейсъра на Сюзан; най-сетне грешките в окабеляването (в оригинала *faulty cabling*) — та как изобщо е работила системата до този момент?

• **паролата на Сюзан** (гл.36) — без да се знае операционната система, под която работи компютърът на Сюзан, не може да се каже каква е минималната дължина на парола, но от текста излиза, че става дума за 5-символна парола. Понеже в английската азбука има 26 букви, ако към тях се добавят и десетте цифри, общият брой на допустимите символи става 36. При дължина на думата/паролата равна на пет, общият брой на възможните комбинации е 36^5 = 60.4 милиона комбинации.

• **терминалите** (гл.36) — Дан Браун отделя голямо внимание на „заключванията“ на терминала и т. н., но предлаганата информация е на нивото на 80-те години. Потенциометри за намаляване на яркостта имаше в старите версии на мониторите от типа VT (може да се предполага, че Сюзан не използва PC в организация, където просто бъка от суперкомпютри). В наше време най-лесният начин да се изгаси монитор, е да се изключи захранването му с бутона. А бавното фокусиране на монитора е нещо напълно непознато за по-младите читатели на тази книга.

• **„сървър за електронна поща“** (гл.36) — объркване на понятията. Съвременната компютърна технология, работата в мрежа и използването на Интернет, предполагат т.н. приложения от вида „клиент — сървър“. Без навлизане в ненужни подробности, „клиентите“ (много на брой) изпращат заявки за обслужване до „сървъра“ (един). Хейл можеше да има на компютъра си „сървър за

електронна поща“, ако беше примерно доставчик на Интернет услуги. Вместо „сървър“ той със сигурност има някакъв „клиент“ (за Windows това типично е програмата Outlook).

• **„Номерът е в полиморфните низове!“** (гл.36 — в оригинала mutation strings) — термин, заимстван за нуждите на адекватния превод от вирусите. Означава „с много форми“, но запазвайки функционалността. При вирусите тази техника се използва, с цел създаване на вирус, чиято сигнатура се променя при всяко негово реплициране, за да се затрудни разпознаването му от антивирусните програми. Антивирусните програми противодействат на свой ред, като изчисляват не контролна сума (примерно като някакъв вид сигнатура), а като анализират изпълнимите файлове за присъствие в тях на код, изпълняващ съмнителни операции (евристично откриване на вирусите).

• **„26000 служители“** (гл.43) — всички числа, които могат да бъдат цитирани за АНС са смайващи, но малко от тях са официално публикувани, поради секретността около тази институция. Ето някои данни, приведени от споменатия изследовател на АНС Джеймс Бамфорд и предполагам валидни към 2001 година: общият брой служители на АНС е 38000 (повече от ФРБ и ЦРУ взети заедно), от които 32000 имат специален допуск за работа на територията на Крипто Сити, паркингът там предлага места за 17000 коли и има обща площ 1300 декара, в комплекса има към 50 сгради и общата им застроена площ е към 650 декара, общата дължина на пътищата е към 50 километра, собствената поща на Крипто Сити разпределя ежедневно 70000 пратки и писма, вътрешната полиция начислява 700 души и АНС разполага със собствен тежковъоръжен (SWAT) отряд за случаи, изискващи използване на оръжие, годишната консумация на електроенергия е над 400 милиона киловатчаса (месечната сметка за електричество е близо 2 милиона долара), а енергопреносната мрежа е с дължина 1000 километра. Само ще отбележа, че в комплекса има собствено кино, банка, билетен център, спортен център, концертна зала и дори… гей клуб. Бюджетът на АНС за 2000–01 година е бил от порядъка на 7 милиарда долара.

• **„Джаба лежеше по гръб, заклещен…“** (гл.61) — в това описание има много неща, които са далеч от реалността. Първо, Джаба е началник отдел Сис-сек (или в казано на прост език „Защита на

компютри“), т.е. той няма работа с поялници, жици, чипове и т.н.; второ, той запоява „нов комплект атенюатори“ (затихватели на сигнала) — такъв компонент в компютрите (където става дума за цифрова, а не аналогова схемотехника) просто отсъства, там проблемът по-скоро е сигналите да се усилят (вместо отслабят, което е задачата на атенюаторите) и двете нива (на логическата „0“ и логическата „1“) да се раздалечат максимално; трето, при суперкомпютрите (а в АНС едва ли има други) изобщо няма такова нещо като „дънна платка“, защото дънната платка е начин за свързване на периферия или най-малкото за осъществяване на връзка между две (или повече) други платки, поставени в куплунзи (слотове) на дънната. При суперкомпютрите (където няма никаква нужда от свързване на периферия) е от значение максималното бързодействие и затова целта е да се намали разстоянието между процесорите, не да се увеличи (което би било резултат от използването на дънна платка); четвърто, абсурдно е да се намери кухина в суперкомпютър, способна да поеме 180 килограмов мъж. Освен това, на подобно ниво на работа (където времето за отстраняване на повреда задължително трябва да е минимално) дефектиралите блокове направо се заменят с други (а повредите се отстраняват не на място, а в лаборатория). Най-сетне възможно ли е някой да лежи под „дънната платка“ (това че е дънна, ако изобщо приемем съществуването й, не я прави автоматично хоризонтална) на суперкомпютър и да запоява чип на ръка с поялник и то не къде да е, а точно в АНС, и не кога да е, а късно събота вечер?

• **„Ще изтрия целия твърд диск… Ще го преформатирам“** (гл.62) — Сюзан би следвало да знае, че изтриването на твърдия диск на компютър, а най-малко от всичко „преформатирането му“ *не* премахва информацията от него. Има специални методи за възстановяване на информация на твърди дискове, сред които например MFM и AFM (**M**agnetic/**A**tomic **F**orce **M**icroscopy), пред които не остава нищо скрито. Нужни са специални програми, които неколкократно записват различни комбинации от данни върху секторите, където трябва надеждно да се изтрие информация, за да може поне донякъде да се разчита, че тя е невъзстановима. А специално „преформатирането“ (както е добре известно) не изтрива нито байт информация от твърдия диск.

• **„… да влезе в терминала на Хейл…“** (гл.64 и на други места) — авторът използва този термин, но „терминал“ по същество означава комбинация от клавиатура и дисплей, свързан по някакъв вид кабел с централен компютър. Терминалът по принцип е бездисково устройство и следователно не може да „помни“ информация. Когато говори за „влизане в терминал“ авторът (вероятно?) има предвид осъществяване на достъп до личната файлова система на даден потребител, която се съхранява на компютъра, който на свой ред може да се намира далеч от терминала. Самото „влизане“ по принцип не е необходимо да става през точно определен терминал (макар да е възможно да се наложи подобно изискване). Така че и форматиране на диска (вж. по-горе) не би било възможно, защото операционната система не би го позволила (най-малкото понеже този диск се ползва от много потребители и какво би станало, ако всеки от тях можеше по желание да го преформатира). Най-многото, което може да се направи, е да се изтрият файловете в дела на потребителя.

• **„…код с ротиращ ключ…“** (гл.75) — поради това, че говори за несъществуващо нещо, авторът непоследователно го нарича с различни имена: в гл.5 и 36 това е „циклично ротиращ открит текст“ (rotating clear text), а тук става дума за код с ротиращ ключ (rotating key-code)

• **„Единственото, което трябва да направим, е да извършим подмяната“** (гл.75) — де да беше толкова лесно. Стратмор (или авторът) забравя, че до този момент вече милиони хора са свалили от сайта на Танкадо оригиналната версия и евентуалната подмяна на файла за сваляне може да засегне само тези, които биха свалили файла след това.

• **„Танкадо не би имал никакви причини да заподозре, че алгоритъмът му в Интернет е подменен“** (гл.75) — и това, уви, не е истина. Първо, размерът на файла със сигурност би се променил, защото каквито и промени да вмъкне АНС в лицето на Стратмор, те едва ли биха били осъществими в точно същия размер на файла. Второ, компютърни хакери от цял свят непрестанно атакуват различни сайтове и често ги разбиват (най-зрелищни са примерите със сайтовете на Белия дом и този на НАСА), след което променят техния облик, а естествено биха могли да променят и достъпните за сваляне от тях файлове ако има такива. Така че Танкадо, чийто сайт имаме основание

да предполагаме е обект на жив интерес, и който сам е бил хакер, несъмнено би имал „едно на ум“ и сигурно би проверявал по всякакви начини дали не е станал жертва на друг хакер (в случая АНС като най-големият възможен хакер).

• **„Колкото по-бързо направим подмяната, толкова по-добре“** (гл.75) — в съзнанието на читателя остава картината, че Сюзан и Стратмор откриват ключовата фраза (каквото и да означава това) сред файловете на Хейл, отварят шифрования файл с „Цифрова крепост“, после Стратмор (който се е трудил месеци наред над нещо, което не е виждал през живота си) вмъква в кода „задна врата“ (сякаш задните врати са нещо стандартно, което се лепи към всичко с едно щракване на пръсти), след това набързо разбиват сървъра със сайта на Танкадо и накрая подменят оригиналния файл с манипулирания. Всъщност, основният проблем е „лепенето“ на „задната врата“. Първо, това явно трябва да се направи незабелязано (защото иначе някой както Хейл при измисления случай със „Скипджак“ ще открие вратата), и второ, няма рецепти за „задни врати“ — реализацията на задна врата зависи от кода, към който тя се инсталира.

• **„Единствената светлина *(над «Крипто» — бел. моя)* идваше от звездите над главите им и слабото излъчване на мониторите зад разбитата стъклена стена на «Възел 3»«** (гл.77) — още едно потвърждение, че забележката за прозрачното покритие (вж. по-горе гл. 4) не е случайна: АНС безгрижно е инсталирала най-могъщия си компютър под едва и не открито небе, удобно за наблюдение от вражеските сателити.

• **»… голяма цвъртяща капка втечнено олово“** (гл.78) — припоят (в оригинал raw solder), използван за запояване на интегрални схеми е на базата на калай, а не олово, защото температурата на топене на калая (~230°C) е с почти 100 градуса по-ниска от тази на оловото. Всъщност, използването на оловен припой (има и такъв и се използва примерно за запояване на медни тръби) би повредило фатално запояваната интегрална схема, преди тя да е заработила.

• **„дванайсетжилен кабел за лазерни принтери“** (гл.85) — към 1996 (и доста преди това), когато е била писана книгата, и по-конкретно в АНС (както във всяка голяма организация), принтерите обикновено се използват като мрежови устройства (за да могат да се ползват не локално от само един компютър, а от повече), което

означава, че се свързват към мрежата с обикновен мрежов кабел (който не е 12-жилен). Другият кабел, нужен за работата на един принтер, също е възможно най-обикновен захранващ. Най-сетне в нито един вариант на използването им за лазерните принтери не са нужни по-особени кабели от тези за другите (мастиленоструйни или по-старите матрични)

• **„ако три милиона силициеви процесори прегрееха и решаха да се възпламенят“** (гл.86) — авторът за втори път споменава за запалване на силиция (вж. също и гл.59 — **„дори може да запалят силициевите чипове“**) — силицият е неметал с точка на топене 1410°C и на кипене 2355°C. Не е известно да *гори* особено добре и може само да се гадае при каква температура може да стане това (*по-късно* добавено от преводача уточнение относно този спорен факт: след доста ровене из Интернет се оказа, че все пак силицият може да гори, при това специфичната топлина, която отделя е по-висока от тази на въглерода (860 kJ/mol срещу 394 kJ/mol), информация за *единствения* документиран случай на горене на силиций — явно става дума за крайно нетипична ситуация — има на http://antoine.frostburg.edu/chem/senese/101/inorganic/faq/silicon-burns.shtml). Горенето е бурно протичаща химическа реакция на свързване с кислород и отделяне на топлина. Единственото, което може да се каже със сигурност е, че още по време на процеса на покачване на температурата до такива нива, първо ще започнат да горят самите платки, да не говорим, че подобна консумация на енергия със сигурност ще накара да сработят прекъсвачите на захранването (каквито просто не може да няма)

• **„TRANSLTR бе разбил с лекота защитната обвивка и бе освободил вируса“** (гл.86) — но ако е така (след като вирусът е зашифрован с достатъчно надежден, но стандартен шифър, неразбиваем от другите), как тогава TRANSLTR не е сигнализирал края на операцията по отварянето му? И после, ако полиморфните низове в основата на „Цифрова крепост“ (за който се е считало, че съществува) са неизползваеми (нали вече няма „Цифрова крепост“) каква все пак е тяхната роля тогава?

• **„Заглушителят му…“** (гл.93) — от предишни глави знаем, че Улохот е въоръжен с револвер (**„Цилиндърът започваше да се завърта…“** — вижда Бекър в гл.81). Поради тази причина с него не

може (просто няма смисъл) да се използва заглушител. Обяснението е, че на мястото, където цилиндърът прави контакт с цевта, винаги има (макар и малка) хлабина, през която излиза част от изгорелите газове. А след като не могат да се уловят всички изгорели газове, не може да има и заглушаване.

• **„Дейвид Бекър изкачи последното стъпало…“** (гл.98) — авторът многократно споменава в тази глава стълбището на „Хиралда“, но допуска малка неточност: „Хиралда“ няма стълбище, а рампа — без стъпала. Построена е от маврите (които били мюсюлмани) и те направили рампата, за да може да се стига лесно и бързо с магарета до върха, когато трябвало да се обяви на правоверните, че е време за молитва.

• **„…титаново-стронциевите процесори…“** (гл.104) — Както и силицият, този материал не може да гори (топи се при 2080°) (виж уточнението по-горе за горенето на силиция). Съединението е известно като стронциев титанат ($SrTi0_3$, създаден през 1953 от Commercial Crystal Labs) и представлява кристален материал с висока диелектрична константа, който сам за себе си не притежава абсолютно никакви попупроводникови свойства; единственото му отношение към микроелектрониката е в това, че може да се използва за подложка, върху която се отлагат тънки свръхпроводящи филми.

• **„Почувства бързото й издигане (*на огнената топка — бел. моя*) в посока на кислорода, освобождаван от горящите чипове“** (гл.105) — горенето е процес на свързване на кислорода (т.е. неговото изчерпване), а не създаване.

• **„Сюзан познаваше тази миризма. Силициев дим“** (гл.107) — интересно откъде й е позната (тя все пак е математик), когато обстоятелствата, при които би могла да вдиша разтопен (още по-малко горящ с изпускане на дим?) силиций, съществуват само в лабораторни реактори на броени места по света.

• **„… изкопани 250 метрични тона земя“** (гл.109) — без да се знае специфичното тегло на изкопаната земя (но едва ли става дума за рохкава пръст), ако приемем занижена стойност от 2 гр/см^3 (само два пъти по-високо от това на водата), явно е, че става дума за обем по-малък от този на двустаен апартамент, което нито позволява разполагането на 12 работни станции (да не говорим, че няма как

групичка техници да „тичат“ от станция на станция), нито монтирането на видеостена с габарити 9/12 метра.

• **„Пред вас е камикадзето на компютърните нашественици — *червеят*“** (гл.109) — Джаба правилно изтъква, че не става дума за вирус, но специално той („полубогът на АНС“) най-добре би би трябвало да знае, че това не е и червей. „Червеят“ е програма, която се разпространява, прониквайки по мрежата като изчислява мрежовите адреси на други компютри, за да им изпрати свое копие. Подобни структури код могат да стартират програми върху системните дискове, но по правило единственият ресурс, до който имат достъп, е оперативната памет на заразения компютър. В случая обаче става дума за типичен „троянски кон“ („троянец“): това е програма, способна на деструктивно действие (наричат я още „логическа бомба“, поради заложената способност да се задейства при настъпване на определени обстоятелства), проникнала под прикритието на друга програма (точно това е описаният случай — проникнала е маскирана като зашифрован вирус).

• **„PEM-базиран прозорец за оторизация“** (гл.110) — PEM е съкращение от **P**rivacy **E**nhanced **M**ail, която (заедно с PGP — от **P**retty **G**ood **P**rivacy) е програма, с чиято помощ двама души могат да си кореспондират по начин, непозволяващ на друг да чете техните имейли и която допълнително удостоверява, че лицето, което изпраща имейла, действително е онова, за което се представя (и двете програми използват алгоритъма RSA). Използването на PEM в дадения контекст е безсмислено, понеже никой от атакуващите хакери не изпраща шифровани имейли до базата данни (самата фраза е комична), за да се минава през някаква оторизация.

• **X11** (гл.110 и 117) — популярно наименование за версия 11 (последен рилийз 6, т.н. X11R6, от май 1994) на графична система с работа с прозорци, използвана в миналото при много UNIX-базирани операционни системи (развитие на предишна система за работа с прозорци, известна като W), при която се реализира специфичен протокол „клиент-сървър“, познат като X-протокол. Тази система се описва като „раздута, претоварена с възможности, функционално усложнена и ненужно тромава“ — изключително малко вероятно да бъде реализирана (точно тя) в инсталирана върху суперкомпютър база

данни (както се описва в романа). Не е никак ясно какво означава нейния срив в резултат от работата на описвания червей.

• **„Четирибитови буквени групи“** (гл.120) — не е ясно какво означава пояснението „четирибитови“. Вътрешното представяне на символите в паметта на компютъра е 8-битово (1-байтово). Много по-важно е друго съображение: разбираме, че в базата данни вършее „троянски кон“, т.е. програма (а не текст), следователно тя трябва да е била вече компилирана (от Танкадо), за да може да изпълни деструктивното си действие. Но ако е така, как тогава са останали в нея „изолираните фрагменти“, които ако нямат отношение (по дефиниция) към останалата част от програмата, няма и да бъдат компилирани до изпълним код в тялото на файла, т.е. изобщо няма как да бъдат намерени в него.

• **„Енигма била 12-тонно чудовище“** (гл.120) — освен, че няма нищо общо с истината, авторът сам си противоречи с написаното в гл 3: **„Външно устройството *(«Енигма» — бел. моя)* напомняло стара пишеща машина“**. 4-буквеното групиране обаче е истина.

• **„Това е Цезаров квадрат“** (гл.121) — вече се спомена (вж. по-горе бележката към гл.3), че това не е „цезаров шифър“.

• **„Простите числа са основни градивни блокове на практически всички алгоритми за зашифроване“** (гл.125) — това твърдение не е вярно: практически *всички* алгоритми за зашифроване не използват математика изобщо и/или прости числа в частност (така е с DES, приетият неотдавна като нов стандарт AES и още десетки или дори стотици подобни), а повечето от съвременните се основават на принципите на Файстел (вж. по-горе в бележките). Авторът има предвид алгоритми като RSA или да кажем Ел Гамал, които са в основата на асиметричните криптосистеми с публично известни ключове, но те се използват най-вече за обмен на сесийни ключове за симетрични (от класически тип) шифри. И изобщо шифрите, използващи резултати от теория на числата (на база теореми, отнасящи се до прости числа), се броят на пръстите на едната ръка (т.е. не са „практически всички“).

• **„Особено подходящи за шифроване ги прави обстоятелството, че компютрите не могат да се справят с тях, използвайки типичните методи за намиране на делители от рода на числовото дърво“** (гл.125) — тук авторът излиза много над сферата

си на компетентност. От казаното излиза, че успехът на алгоритмите, използващи прости числа, е в неспособността на компютрите да ги разложат на множители (уточнението, че не могат да го направят с традиционните методи е още по-нелепо, защото простите числа се неразложими на делители с каквито и да са методи — те са „прости“ точно защото нямат делители). Истината е по-различна: за един алгоритъм като RSA, типичен представител на групата шифри, използващи теореми от теорията на числата, един от компонентите на шифъра е *съставно* число, произведение на две много големи прости числа. Разбиването на шифъра е възможно, ако се знаят делителите, но при дължини от стотици цифри (за всеки прост множител) *всички* засега известни методи изискват астрономически голям брой операции, което обезсмисля масовото им прилагане и гарантира надеждност на шифъра поне в средносрочен план.

• **за бележката под линия в края на гл.126**: в тази бележка под линия със сигурност има някаква грешка — стойностите не само, че не са близки, те са *астрономически* различни — единият множител е 10^{134}, което е число по-голямо от предполагаемия брой на протоните в цялата Вселената, а другият е над 10^{100} пъти по-малък, освен това няма никакви размерности. Въобще числата са толкова различни, че използването на знаци след десетичната запетая е безсмислено (силно опростен пример би било да сравняваме 1,00091 и 10 милиарда — за какво ни е точността в представянето на първото число? А в книгата става дума за направо несъпоставими числа). На всичко отгоре при възможна грешка от порядъка на 12%, няма никакъв смисъл да се изписва едно число с точност до стохилядните, когато смисълът на бележката е, че това число е вярно с точност до единиците (колкото е приблизително 12% от 10).

ЗАСЛУГИ

Имате удоволствието да четете тази книга благодарение на *Моята библиотека* и нейните всеотдайни помощници.

http://chitanka.info

Вие също можете да помогнете за обогатяването на *Моята библиотека*. Посетете **работното ателие**, за да научите повече.