EVERYDAY ENCRYPTION = KAŽDODENNÍ ŠIFROVÁNÍ (Sandra Kas Miller)
http://www.securitysolutions.com/mag/security_everyday_encryption/index.html

Encryption is being implemented in many places besides the office. Most people associate encryption with protecting information as it travels across a network or as a means to secure data storage; however, it actually touches just about every facet of our everyday life. The word encryption once conjured up images of covert diplomatic communication and secret codes to which only a select few were allowed access. But the rise of the Internet age and increasing theft of private digital information have thrust encryption technologies into the public spotlight.
While the average user might not know an algorithm from a protocol, they do understand that the online banking Web site they visit has been secured. For the truly paranoid, Web browsers now offer single-click access to view the certificate issued by a trusted third party Certificate Authority, which certifies that the Web site is official — not a "look-alike" page designed to steal logon and password information. Viewing the certificate is as simple as clicking on the lock icon, for example, that usually appears to the right of an active URL box on a PC's Web browser. This opens a certificate viewer that will provide ample information about the certificate, such as who issued the certificate and to whom, how long it will be valid, information about the algorithms used and the type of encryption. These implementations of encryption are obvious, but there are more subtle ways in which encryption enters our daily lives.

Šifrování je realizováno na mnoha místech mimo kancelář. Většina lidí spojuje šifrování s ochranou informací jako je posílání dat sítí nebo jako prostředek pro bezpečné uložení dat; ale toho se vlastně dotýká téměř každý aspekt našeho každodenního života. Slovo šifrování jednou vykouzlil obraz tajných diplomatických komunikací a tajné kódy, ke kterým byl povolen přístup jen pár vyvoleným. Ale rozmach internetového věku a rostoucí zcizování privátních digitálních informací posunulo šifrovací technologie do pozornosti veřejnosti.
Zatímco průměrný uživatel nemusí znát algoritmy protokolu, stačí, že chápe, že webové stránky jeho on-line bankovnictví, které navštěvuje, jsou zabezpečeny. Pro opravdové paranoiky webové prohlížeče nyní nabízí jedním kliknutím přístup k prohlédnutí osvědčení vydané důvěryhodnou třetí stranou, certifikačním úřadem, která certifikuje, že webová stránka je oficiální a stránky nejsou navrženy jako „jiné podobné"´tak, aby bylo možno krást přihlašovací jména a hesla.
Prohlížení osvědčení je stejně jednoduché jako kliknutí na ikonu zámku, například to, že se obvykle objeví na pravé straně řádku s URL adresou v okně webového prohlížeče. Tím se otevře prohlížeč ověření, který bude poskytovat dostatečné informace o osvědčení (jako například kdo vydal osvědčení a komu, do kdy bude platit, informace o způsobu použití a o typu šifrování). Toto zavedení šifrování je jasné, ale existuje více zajímavých způsobů, jak šifrování vstupuje do našeho každodenního života.

An average day
Your day starts out with watching a few minutes of news and weather on satellite television prior to heading out for a morning job, which is now more pleasant thanks to your iPod. A little while later, you head out to work, arming your house alarm as you walk out the door. You open the door to your car with a keyless lock numeric pad and start your morning commute. After a quick stop for fuel, paid for at the pump with a credit card, you hop on the toll road in the fast lane using a SpeedPass that automatically deducts the toll from your pre-paid account. At the office, you turn on the computer, finally becoming cognizant of encryption, when logging on to the network using either a password or some type of physical token. However, you remain oblivious to the half dozen instances of encryption that have already touched your life so far today.

Průměrný den
Váš den začíná několikaminutovým sledováním zpráv a počasí v satelitní TV jako hlavní ranní činnosti, které jsou teď mnohem příjemnější díky našemu iPodu. O několik minut později můžete vyrazit do práce, procházíte dveřmi sledováni vaším domácím alarmem. Otevřete dveře vašeho auta číselnou klávesnicí vašeho dálkového ovládače a začínáte cestu do práce. Po krátkém zastavení pro palivo, které zaplatíte u pumpy vaší kreditní kartou, se můžete rychle přesunout do rychlého pruhu silnici

díky kartě SpeedPass, ze které se odečte mýtné z vašeho předplaceného konta. V kanceláři zapnete počítač a konečně přichází vědomí šifrování, když se přihlašujete do sítě buď jménem, nebo nějakou čtečkou fyzických údajů. Nicméně můžete zůstat lhostejní k půl tuctu šifer, které se vás dotýkají, je ještě daleko den, kdy to bude dokonalé.

"I really see encryption as glue. You have a lot of things that are held together by glue but you don't really see it. It's important that it works well, otherwise everything falls apart," explains Nate Lawson, senior researcher at Cryptography Research, and adds they would work with a company making SD [Secure Digital] cards and help them to integrate security into their product because Cryptography Research is unique in that. It does not necessarily sell a product, but helps manufacturers integrate encryption technologies into their electronics.

„Opravdu vidím, že šifrování je jako spojení. Máš mnoho věcí, které jsou takto spojeny, ale ve skutečnosti to nevidíš. Je důležité, že to funguje/pracuje, jinak se všechno rozpadne," vysvětluje Nate Lawson, vedoucí vědecký pracovní v kryptografii a dodává, že by měli pracovat pro firmu vyrábějící SD karty a pomáhat jim se zavedením ochrany do jejich produktů, protože Cryptography Research je v tomto výzkumu jedinečná. Není nezbytné prodávat produkt, ale pomoci výrobcům zavádět šifrovací technologie do jejich elektroniky.

Purchasing and using electronics is not the only way encryption creeps into our daily lives. As of August 2006, anyone obtaining a U.S. Passport will have their photograph digitized and stored along with their personal information on a contactless computer chip embedded in the cover. Readers in close proximity can only read the e-passports, and they also possess an integrated encryption engine much stronger than the one used in the inexpensive RFID tags for supply chain management.
To put e-passport security in perspective, Jim Handy, an analyst at Semico Research, a semiconductor research company based in Phoenix, says "Getting into these chips is going to take more than your average bear. There will be MIT students who do it, but it probably won't be widespread. You'll have to know how the chip is encrypted and how it is programmed."
Many countries have started issuing e-passports since then and by 2010 citizens from nearly 200 countries will be carrying passports containing an encrypted computer chip storing their image and personal information.

Nákup a použití elektroniky není jediný pouze způsob, jak se šifrování vloudí do našeho každodenního života. Pokud chce někdo od srpna 2006 získat americký pas, jeho fotografie bude digitalizována a uložena společně s jeho osobními údaji do bezdotykového počítačového čipu zabudovaného v obalu. Čtenáři z bezprostřední blízkosti mohou pouze číst e-passports, a také mají integrované šifrování mnohem silnější, než bylo použito v levných RFID visačkách pro řízení dodavatelského řetězce.
V e-pasu je perspektiva zabezpečení, Jim Handy, analytik z Cryptography Research, výzkum polovodičů se sídlem v Phoenix říká: „Dostat se do těchto čipů bude trvat mnohem déle než váš průměrný život. Budou zde studenti MIT, kteří to udělají, ale pravděpodobně se to nerozšíří. Budete vědět, jak je čip šifrován a jak je naprogramován.
Mnoho zemí již začalo vydávat e-pasy a do roku 2010 budou občané přibližně 200 zemí nosit pasy obsahující zašifrovaný počítačový čip obsahující jejich podobu a osobní informace.

Digital rights and anti-tampering
Regulatory compliance has brought the question of whether or not organizations employ encryption to a new level of awareness, but there is another side to the growing use of encryption — anti-piracy and product tampering. There has been a sharp rise in the number of companies who are integrating encryption into their core components, especially when it comes to tamper-resistance. According to Lawson, encryption is becoming increasingly common in consumer devices. "Typically, you think of servers, network links and hard drives, but now, even the smallest of devices, including

microcontrollers, are getting crypto support for doing things like secure boot so manufacturers know what software is being loaded into the processor."
Historically, everything was stored on a single chip, which could be reverse-engineered by disassembling the chip to find out how it works. Now, the stakes are higher with the dependence on software. "Software is becoming so valuable because it is easy to copy, patch and update," Lawson explains, "The problem is people are hacking their iPods to run Linux."
To alleviate the problem, companies want to essentially lock out access to the devices, prevent modifications to the software or stop users from taking the software from one device and using it in another. The satellite cable industry can be cited as an example – once you decrypt a broadcasted signal, you can watch its stuff free forever. It is estimated that satellite companies and the channels, movie studios and sports franchises that supply programming lose well over $1 billion a year in uncollected revenue from piracy. To help combat the loss, Cryptography Research has been involved in helping satellite television companies by developing an applicationspecific integrated circuit (ASIC).
The entertainment industry has embraced cryptographic technologies in recent years, even showing up on the agenda at the RSA convention in 2005 to reach out to IT companies for developing better anti-piracy technologies. Better known as Digital Rights Management (DRM), it is now routinely found on music CDs and movie DVDs. Apple constructed FairPlay, the DRM that digitally encrypts audio files so they can only be played using iTunes or an iPod. Rarely does anyone consider the fact that their iPod contains its own encrypted key repository.
The latest frontier for encryption in the entertainment industry has been for high-definition (HD) movies. Disney, Intel, Microsoft, Panasonic, Warner Brothers, IBM, Toshiba and Sony have worked together to develop the Advanced Access Content System (AACS) — encryption for protecting HD formats such as Toshiba's HD DVD and Sony's Blu-ray Disc. Less than six months after AACS was put into production, a hacker had already posted the crack online. That is why many who work in the field of cryptography refer to it as a "race" rather than a solution.
Encryption schemes based upon renewability are what Lawson sees as the next step. "Once someone compromises the system, a new update can be issued and the system becomes secure again," he says. "Such encryption is gaining use in familiar electronics such as cell phones, home office routers, digital video recorders and many other consumer electronics.
"I think we've seen large increases in the use of encryption," points out Gartner, vice president and research fellow, John Pescatore. "But how much of it people realize they are using remains transparent."

Digitální práva a odolnost proti ilegálním zásahům
Dodržování právních předpisů přineslo otázku využití šifrování v nové rovině povědomí, ale je zde i druhá s rostoucím využitím šifrování – anti-pirátství a falšování produktů. Došlo k ráznému vzestupu počtu firem, které začleňují šifrování do svých hlavních komponentů, zejména pokud jde o zabránění zneužití. Podle Lawsona, šifrování se stále více dostává do spotřebitelských zařízení. „Typicky si myslíte, že pro servery, síťová spojení a pevné disky, ale nyní jsou to i ta nejmenší zařízení, včetně mikrořadičů, které dostávají šifry pro podporu činností jako bezpečné spuštění, takže výrobci vědí, jaký software se nahraje do procesoru."
Historicky, vše bylo uloženo na jednom čipu, který by mohl zpětně rekonstruovat funkčnost čipu, který by byl demontován. Nyní je v sázce vyšší závislost na softwaru. „Software se stává stále cennějším, protože se snadno kopíruje, opravuje a aktualizuje," vysvětluje Lawson, „problém je, že lidé jsou hackování svými IPody běžícími v Linuxu."
Ke zmírnění problém chtějí firmy zásadně omezit přístup do svých zařízení, předejít změnám softwaru nebo zabránit uživatelům v braní softwaru ze zařízení a použít jej v jiném. Satelitní kabelový průmysl může být citován jako příklad – jakmile byl dešifrovaný vysílaný signál, můžete programy sledovat kdykoli volně. Odhaduje se, že satelitní společnosti a kanálů, filmová studia a sportovní licence, které dodávají programy, tratí kolem jednoho bilionu dolarů ročně za nevybrané poplatky z

důvodu pirátství. K pomoci v boji proti ztrátě byl Cryptography Research zapojen do pomoci satelitním televizním společnostem tím, že vyvíjí aplikovaný integrovaný obvod (ASIC).
Zábavní průmysl uchopil šifrovací technologie až v posledních letech, kdy ukazovala na agendy úmluvy RSA v roce 2005 informovat IT společnosti pro vývoji lepších anti-pirátských technologií.
Více známý jako Digital Rights Management (DRM), který je nyní běžně k dispozici na hudebních CD a filmových DVD. Apple se zachovalo Fair Play, DRM, které digitálně šifruje zvukové soubory tak, že mohou být přehrávány pouze pomocí iTunes nebo iPod. Výjimečně se někdo zamyslí nad tím, že jeho iPod obsahuje vlastní šifrovací klíč schránky.
Poslední hranice šifrování v zábavním průmyslu byly pro HD filmy. Disney, Intel, Microsoft, Panasonic, Warner Brothers, IBM, Toshiba a Sony pracovali společně na vývoji Advanced Access Content System (AACS) – šifrování pro ochranu HD formátů jako je třeba Toshiba HD DVD nebo Sony Blue-ray Disc. Ani ne 6 měsíců, co byl AACS uveden do výroby, byli již hackeři dobře informováni. To je důvod, proč mnoho lidí pracujících v oblasti šifrování toto označují jako „závod“ spíše než řešení.
Šifrovací systémy založené na obnovitelnosti je to, co Lawson vidí jako příští krok: „Jakmile někdo ohrožuje systém, může být vydána nová aktualizace a systém se stane opět bezpečným,“ říká. „Takové šifrování získává použití v běžné elektronice jako jsou mobilní telefony, směrovače domácí kanceláře, digitální video přehrávače a mnoho další spotřební elektroniky.“
Myslím, že jsme viděli stále se zvětšující použití šifrování,“ upozorňuje Gartner, víceprezident a výzkumný spolupracovník Johna Pescatore. „Ale kolik lidí si uvědomí, jak je použití i nadále průhledné.“

Help

conjure up translation: vybavit (si), vyvolat, vyvolávat, evokovat
explanation: to bring into the mind or caused to be remembered, evoke
vykouzlit, vytvořit obraz v mysli, k výrobě jakoby odnikud
(synonyma: vychovávat, vykouzlit, vyvolání, vyvolat, předložila, probudit, evokují, zamíchat, zvýšit)

facet translation: stránka, aspekt
explanation: a facet of something is a single part or aspect of it; any of the many parts of a subject to be considered
aspekt něčeho, jako je osobnost, odlišný rys či prvek problému
(synonyma: aspekt, charakteristika, funkce, boční, sektor, sféra)

tamper-resistance
translation: odolnost proti ilegálním zásahům
explanation: resistance to tampering either the normal users of a product, package, or system or others with physical access to it
odolnost proti ilegálním zásahům - odolnost vůči běžnému uživatelskému výrobku, balíčku nebo systému nebo čemukoli jinému s fyzickým přístupem k němu. Manipulační odpor se pohybuje od jednoduchých prvků, jako jsou šrouby se speciální hlavou k více složitým zařízením, která je činí sama nefunkční nebo šifrovat veškerá data přenosy mezi jednotlivými čipy.
Odolná zařízení nebo funkce jsou také běžně balená, aby odradila od manipulace s výrobkem.

compliance translation: shoda, harmonie, vyhovení cemu, poddajnost
explanation: obedience to a rule, agreement, demand, etc.; the tendency to agree willingly to other people's wishes or demands
shoda - akt v souladu s přáním, dotaz, nebo požadavek, souhlas, dispozice nebo tendence ustoupit druhým; prodloužení nebo posunutí načtení struktury z jednotky; flexibilita.

revenue translation: příjem, tržba, výnos, státní důchod
explanation: income, esp. that which the government receives as tax
příjmy - příjmy ze všech vládních zdrojů vyčleněných pro vyplacení příspěvku z veřejných výdajů; výnos z majetku nebo investice; příjem
(synonyma: částka, množství peněz, suma, částka peněz, daně z příjmu, daně)

combat translation: boj, konflikt, zápas; bojovat, zápasit, potírat; bojový, bitevní
explanation: a struggle, a fight
boj
sl. oponovat v boji, bojovat proti, důsledně oponovat; bojovat proti
(synonyma: boj, zápas, potýkat se)
p. jm. boj, především vojenské bitvy, sváry (synonyma: bitva, střetnutí, boj, konflikt)

ample translation: dostatecný, hojný, bohatý, postacující
explanation: enough, or more than enough
dostatek - z rozsáhlé nebo velké velikosti, množství, rozsah nebo kapacita; velký stupeň, druh nebo množství; víc než dost; plně dostačující k uspokojení potřeby nebo účelu
(synonyma: hojný, dostatečné, hojný, hojný, hojný, bohatý)

toll translation: poplatek, právo vybírat poplatek
explanation: money that you pay to use something
mýtné
p. jm. fixní poplatek nebo daň za privilegium, zejména pro průjezd přes most nebo po silnici, poplatek za služby, množství nebo rozsah ztráty nebo zničení života, zdraví nebo majetku
(synonyma: poplatek, cena, náklady, hodnoty)
sl. k přesné jako mýtné, účtovat poplatek za užívání
(synonymum: uložit)

EVERYDAY ENCRYPTION = KAŽDODENNÍ ŠIFROVÁNÍ (Sandra Kas Miller)
http://www.securitysolutions.com/mag/security_everyday_encryption/index.html

A. Vocabulary

1. Spojte slova s jejich významem

1. plaintext (cleartext)
původní, čistý text

A. encoding the contents of the message in such a way that hides its contents from outsiders
šifrování obsahu zprávy takovým způsobem, že je zasílaný obsah skrytý

2. non-repudiation
neodmítnutí

B. the art or science of mathematical techniques related to aspects of data security
umění nebo věda matematických technických postupů souvisejících s aspekty zabezpečení dat

3. encryption
šifrování, kódování

C. the process of retrieving the plaintext from the ciphertext
proces získávání původního textu z šifrovaného textu

4. confidentiality
důvěrnost, utajení, zachování důvěrnosti

D. a coding method
metoda kódování

5. cryptanalysis
kryptoanalýza, dešifrování

E. an aspect of data security, detecting the unauthorized alteration of data
hledisko (aspekt) zabezpečení dat, detekce neoprávněné (neautorizované) změny dat

6. cryptology
kryptologie

F. an aspect of data security, identifying either entities or data origins
hledisko zabezpečení dat, určení subjektů nebo data vzniku

7. key
klíč

G. an aspect of data security, preventing an entity from denying previous commitments or actions
hledisko zabezpečení dat, předcházení odmítnutí předchozích závazků nebo akce

8. cryptography
kryptografie, šifrování, kódování

H. a message to a receiver
zpráva pro příjemce

9. ciphertext
šifrovaný text

I. the study of mathematical methods which are used in attempting to defeat cryptographic techniques
studium matematických metod, které jsou užívány při pokusech zvládnout šifrovací techniky

10. data integrity
integrita dat, neporušenost údajů

J. the study of cryptography and cryptanalysis
studium kryptografie a kryptoanalýzy

11. decryption
dekódování, dešifrování

K. an encrypted message
zašifrovaná zpráva

12. authentication
autentizace

L. an aspect of data security, keeping secret the content of information from unauthorized parties
hledisko zabezpečení dat, udržení tajného obsahu informace před neoprávněnými osobami

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
H	G	A	L	B	I	D	J	K	E	C	F

2. Complete the text with appropriate terms
divided (9)***, at*** (10)***, decryption*** (1)***, on*** (2)***, knows*** (15)***, derived*** (8)***, method*** (3)***, key*** (4)***, site*** (14)***, that*** (6)***, there*** (5)***, keeping*** (16)***, different*** (7)***, bits*** (11)***, encrypt*** (12)***, public-key*** (13)

Basic Cryptographic Algorithms
The method of encryption and ***decryption*** (1) is called a cipher.
Some cryptographic methods rely ***on*** (2) the secrecy of the encryption algorithms; such algorithms are only of historical interest and are not adequate for real-world needs.
Instead of the secrecy of the ***method*** (3) itself, all modern algorithms base their security on the usage of a key; a message can be decrypted only if the ***key*** (4) used for decryption matches the key used for encryption.
There (5) are two classes of key-based encryption algorithms, symmetric (or secret-key) and asymmetric (or public-key) algorithms.
The difference is ***that*** (6) symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), where as asymmetric algorithms use a ***different*** (7) key for encryption and decryption, and the decryption key cannot be ***derived*** (8) from the encryption key.
Symmetric algorithms can be ***divided*** (9) into stream ciphers and block ciphers.
Stream ciphers encrypt a single bit of plaintext ***at*** (10) a time, whereas block ciphers take a number of ***bits*** (11) (typically 64 bits in modern ciphers), and ***encrypt*** (12) them as a single unit.
Many symmetric ciphers are described on the algorithms page.
Asymmetric ciphers (also called ***public-key*** (13) algorithms) permit the encryption key to be public (it can even be published to a ***site*** (14)), allowing anyone to encrypt with the key, where as only the proper recipient (who ***knows*** (15) the decryption key) can decrypt the message.
The encryption key is also called the public key and the decryption key the private key.
The security provided by these ciphers is based on ***keeping*** (16) the private key secret.

Základní kryptografické algoritmy
Metoda šifrování a **dešifrování** (1) se nazývá kód.
Některé kryptografické metody spoléhají **na** (2) bezpečnost šifrovacích algoritmů; například algoritmy mají pouze historického význam a nejsou dostatečné pro použití v reálném světě.
Aby **metoda (3)** byla bezpečná sama o sobě, mají všechny moderní algoritmy založeny svou bezpečnost na použití klíče; zpráva může být dešifrována pouze tehdy, pokud je pro dešifrování použit **klíč (4)** odpovídající klíči použitému pro šifrování.
Existují (5) dvě třídy základních klíčů šifrovacích algoritmů, symetrické (neboli tajný klíč) a asymetrické (neboli veřejný klíč) algoritmy.
Rozdíl je, že symetrické algoritmy užívají stejné klíče pro šifrování a dešifrování (nebo dešifrovací klíč je snadno odvozen ze šifrovacího klíče), zatímco asymetrické algoritmy užívají **rozdílný (7)** klíč pro šifrování a dešifrování a dešifrovací klíč nemůže být **odvozen (8)** z šifrovacího klíče.
Symetrické algoritmy se **rozdělují (9)** na proudové šifry a blokové šifry.
Proudové šifry šifrují jednotlivé bity ze základního textu **v (10)** čase, zatímco blokové šifry berou počet **bitů (11)** (typicky 64 bitů v moderním šifrování) a jejich **šifry (12)** je jako celek.
Mnoho symetrických šifer je popsáno na stránce algoritmů.

Asymetrické šifry (nazývané **veřejný klíč (13)** algoritmů) dovolují šifrovací klíč zveřejnit (dokonce může být zveřejněn na **webové stránce (14)**), což povoluje komukoli zašifrovat s klíčem, zatímco jen správný příjemce (ten, kdo **zná (15)** dešifrovací klíč) může zprávu dešifrovat.
Šifrovací klíč se také nazývá veřejným a dešifrovací klíč soukromý klíčem.
Zabezpečení poskytování těmito šiframi je založeno na **udržení (16)** soukromých klíčů v tajnosti.

B. Text comprehension

1. Decide whether the following statements are true or false. If false, explain why.
a. A certificate viewer provides ample information about the certificate but the access to it is not open to public.
Certifikát prohlížeče poskytuje podrobnou informaci o osvědčení, ale přístup k němu není veřejný.
~~T~~ F

b. Purchasing and using electronics is practically the only way encryption creeps into our daily lives.
Nákup a užití elektroniky je prakticky jediný způsob jak se šifrování dostává do našeho našeho denního života. ~~T~~ F

c. There has been a sharp rise in the number of companies who are integrating encryption into their core components, especially when it comes to tamper-resistance.
Došlo k prudkému násrutu počtu firem, které využívají šifrování ve svých základních komponentech, zejména pokud jde o odolnost proti ilegálním zásahům. T ~~F~~

d. Some entertainment industry companies have worked together to develop the Advanced Access Content System (AACS) — encryption for protecting HD formats.
Některé společnosti zábavního průmyslu pracovali společně na vývoji AACS – šifrování pro ochranu HD formátů. T ~~F~~

2. Answer the questions.
a. What do most people associate encryption with?
Co si většina lidí spojuje s šifrováním?
On-line banking.

b. Does encryption touch many aspects of our everyday life?
Dotýká se šifrování mnoha aspektů našeho každodenního života?
Yes.

c. If your previous answer was yes, explain where and how.
Pokud vaše předchozí odpověď byla „ANO“, vysvětli kde a jak.
Payment of banking card, shopping, using elektrincs machines, PC, cell phone, home alarm, car, etc.

d. How is it certified that a web site is official?
Jak je to s ověřením, že webová stránka je oficiální?
There is certifikate on the right corner in URL box on web site.

e. How many countries will have issued e-passports by 2010?
Kolik zemí bude v roce 2010 vydávat e-pasy?
Perhaps 200 countries

f. Why do companies – and this trend is still increasing – integrate encryption into their core components?
Proč společnosti – a tento trendy se stále zvyšuje - začleňují šifrování do svých základních komponentů?
It is for better tamper-resistance and opposite unautorized use dates and machines.

g. What does DRM stand for and why was it developed?
Co stojí za DRM a proč byl vyvinut?
Better known as Digital Rights Management (DRM), it is now routinely found on music CDs and movie DVDs. Apple constructed FairPlay, the DRM that digitally encrypts audio files so they can only be played using iTunes or an iPod. Rarely does anyone consider the fact that their iPod contains its own encrypted key repository.

h. Which companies have worked together to develop AACS?
Které společnosti pracují společně na vývoji AACS?
Some companies of entertainment industry – Disney, Toshiba, Warner Brothers, Sony, ...

3. Explain *(Vysvětlete)*

a. What did Lawson mean by the following statement? "I really see encryption as glue."
Co měl Lawson na mysli následujícím výrazem? „Opravdu vidím šifrování jako spojení."
We have a lot of things that are held together by glue but you don't really see it. It's important that it works well, otherwise everything falls apart

b. Why do people working in the field of cryptography refer to it as a "race?"
Proč lidé pracujícá na vývoji šifrování říkají, že je to „závod"?
Becouse after AACS was put into production, a hacker had already posted the crack online.

c. How can users be stopped from taking the SW from one device and using it in another?
Jak lze uživatelům zabránit přenášet SW z jednoho zařízení a používat je na jiném?
digitally encrypts audio files so they can only be played using iTunes or an iPod, rarely does anyone consider the fact that their iPod contains its own encrypted key repository

C. Lexis

1. Use antonyms of the words given in bold and fill them in the sentences.
a. There has been a sharp **fall** in the number of companies who are integrating encryption into their core components.

b. I hate extreme temperatures, I prefer **fixed** ones.

2. Use synonyms of the words given in bold and fill them in the sentences.
a. Absorbed in her work, she was totally **unaware** of her surroundings**.**
*Byla zaujata svojí prací tak, že **nevnímala** své okolí.*

b. These implementations of encryption are **evident**, but there are more subtle ways in which encryption enters our daily lives.
*Tyto implementace kódů jsou **zjevné**, ale je mnoho důvtipnějších způsobů, kterými kódování vstupuje do našich denních životů.*

c. A certificate viewer will provide **ample** information about the certificate, such as who issued the certificate and to whom, how long it will be valid, etc.

*Prohlížečem certifikátu provozovatel **podrobně** informuje o certifikátu, např. komu byl vystaven a kým, jak dlouho bude platit atd.*

d. You should consider various **facets** of the problem before solving it.
*Měli byste zvážit různé **aspekty** problémy před jeho řešením.*

e. Several companies, for **example** Disney, Intel, Microsoft, Panasonic, Warner Brothers, IBM and Sony, have worked together to develop the Advanced Access Content System (AACS) — encryption for protecting HD formats.
*Několik firem, **například** Disney, Intel, Microsoft, Panasonic, Warner Brothers, IBM a Sony, společně pracují na vývoji AACS – šifrování pro ochranu HD formátů.*

f. She did exactly what she promised. I am sorry I **doubted** her.
*Udělala přesně to, co slíbila. Mrzí mě, že jsem o ní **pochyboval**.*

g. We were informed about new government strategies **to fight** inflation.
*Byli jsme informováni o nové vládní strategii **v boji** proti inflaci.*

3. Nouns *(podstatná jména)***, adjectives** *(přídavná jména)* **and verbs** *(slovesa)* **are parts of speech which can be formed by various suffixes. Sort the following suffixes out according to which part of speech they belong. Find a word for each suffix.**
Podstatná jména, přídavná jména a slovesa jsou slovní druhy, které mohou být tvořeny různými příponami. Třídí se podle toho, do které části řeči patří. Najdi slova pro každou příponu.

Suffix *(přípona)*	**Part of speech *(slovní druh)***	**Word *(slovo)***
-ify	**verb**	**identify**
-or		
-ise		
-ible		
-ment	**noun**	**goverment**
-al		
-ship		
-ful		
-er	**adjuctive**	**better**
-ize		
-less	**adjuctive**	**contactless**
-tion	**noun**	**action**
-y		
-able		
-ance		
-ing	**verb**	**coming**
-ive		
-ious		
-en		
-ed	**verb**	**waited**
-ence		

EVERYDAY ENCRYPTION = KAŽDODENNÍ ŠIFROVÁNÍ (Sandra Kas Miller)
http://www.securitysolutions.com/mag/security_everyday_encryption/index.html

Facultative exercises:

1. Translate into Czech
Preface
By encryption, we mean a process of converting information to a disguised form in order to send it across a potentially unsafe channel. The reverse process is called decryption. Using strong encryption techniques, sensitive, valuable information can be protected against organized criminals, malicious hackers, or spies from a foreign military power, for example. Indeed, cryptography used to be almost exclusively a tool for the military.

Šifrováním, máme na mysli proces převodu informací do skryté formy, aby jej bylo možno poslat přes potenciálně nebezpečný kanál. Opačný proces se nazývá dekódování. Pomocí důsledného šifrování, lze citlivé a cenné informace chránit například proti organizované trestné činnosti, zlomyslným hackerům nebo vyzvědači z cizí vojenské síly. Ve skutečnosti, kryptografie býval téměř výlučně nástroj pro armádu.

However, in moving into an information society, the value of cryptography in everyday life in such areas as privacy, trust, electronic payments, and access control has become evident. In this way, the field of cryptography has broadened from classical encryption techniques into areas such as authentication, data integrity, and nonrepudiation of data transfer.

Nicméně, ve směru do informační společnosti, je zřejmá hodnota kryptografie v každodenním životě, například v oblasti soukromí, důvěryhodnosti, elektronické platby a řízení přístupu. Tímto způsobem, se kryptografie rozšířila od klasických technik šifrování v oblastech, jako je autentizace, integrita dat, nepopiratelnost a přenos dat.

2. Complete the text with appropriate terms
The entertainment **industry** has embraced cryptographic **technologies** in recent years, even showing up **on** the agenda at the RSA convention in 2005 to reach out to IT **companies** for developing better **anti-piracy** technologies. Better known as Digital Rights Management (DRM), it is now routinely **found** on music CDs and movie DVDs. Apple constructed FairPlay, the DRM that digitally **encrypt** audio files so they **can** only be played using iTunes or an iPod. Rarely does anyone consider **the** fact that their iPod contains its own encrypted **key** repository.

Zábavní průmysl uchopil šifrovací technologie až v posledních letech, kdy ukazovala na agendy úmluvy RSA v roce 2005 informovat IT společnosti pro vývoji lepších anti-pirátských technologií.
Více známý jako Digital Rights Management (DRM), který je nyní běžně k dispozici na hudebních CD a filmových DVD. Apple se zachovalo Fair Play, DRM, které digitálně šifruje zvukové soubory tak, že mohou být přehrávány pouze pomocí iTunes nebo iPod. Výjimečně se někdo zamyslí na tím, že jeho iPod obsahuje vlastní šifrovací klíč schránky.

FOR YOU:
Presentation Topics
a. Digital Signature
b. Cryptographic Hash Functions
c. Cryptographic Random Number Generators
d. Strength of Cryptographic Algorithms
e. Cryptanalysis and Attacks on Cryptosystems
f. Tamper-resistance

See for example:
http://www.ssh.com/support/cryptography/introduction or www.cryptography.com