Ukázka z kapitoly *1. Abychom si rozuměli …*

Dešifrování

Dešifrování je opačný proces k šifrování. Jedná se o rekonstrukci původního otevřeného textu zprávy z šifrového textu pomocí domluvené kryptografické metody a znalosti příslušného klíče.

Dešifrování provádí zpravidla zamýšlený příjemce zprávy, který tuto zprávu dešifruje pomocí domluvené kryptografické metody a znalosti příslušného klíče. Bývá to většinou šifrant nebo šifrér. Může je však provádět i neoprávněná osoba, která se dostala k příslušnému klíči použitého šifrového systému. Klíč mohl být získán např. pomocí špionáže, ztrátou apod.

Luštění

Kryptoanalytici se snaží získat ze zašifrované zprávy její původní podobu – otevřený text. Cílem však může být i získání alespoň části skrytých informací.

Tento proces hledání se nazývá **luštění šifrové zprávy** a pokud je kryptoanalytik úspěšný a podaří se mu vniknout do některého šifrového systému, řekneme, že šifra byla **zlomena** nebo **rozbita**, slangově „**brejknuta**“ (z anglického break). Prolomení se týká celého šifrovacího systému, tj. od tohoto okamžiku umí luštitel přečíst všechny zachycené šifrové zprávy. Může se však stát (zvláště u kvalitnějších systémů), že luštitel vyluští jen jednu konkrétní šifrovou zprávu, ale tato jeho metoda ještě neumožňuje automaticky přečíst všechny další zprávy. Metoda např. může pomoci proniknout do systému jen za určitých podmínek (slabé klíče, opakované použití stejného klíče, délka šifrové zprávy) nebo při určitém nastavení šifrovacího stroje (nevhodné nastavení směnných prvků).

Dešifrování × luštění

Tato dvě slova neznamenají totéž, i když cílem obou procesů je získat k šifrovému textu odpovídající otevřený text. **Dešifrování** provádí ten, kdo zná všechny potřebné informace k převodu šifrového textu na otevřený tvar, zatímco **luštění** provádí kryptoanalytik (nezamýšlený příjemce), který se snaží získat informace ze zašifrované zprávy bez znalosti klíče a případně i šifrového systému.

Šifry a kódy

Budeme rozlišovat mezi šiframi a kódy. Pomocí **šifry** nebo přesněji šifrovacího systému se odesílatel a adresát snaží utajit obsah zprávy před nepovolanou osobou. Smyslem **kódu** není

zprávu utajit, ale upravit ji tak, aby ji bylo možné dále příslušným technickým prostředkem zpracovávat, např. přenést nějakým kanálem. Kódovaná zpráva tedy může být na základě znalosti příslušného kódování převedena zpět do původního tvaru.

Mezi nejznámější příklady kódu patří ASCII kód a Morseova abeceda. ASCII je využíván zejména ve výpočetní technice jako kód, který nahrazuje jednotlivá písmena a další symboly pomocí posloupnosti 8 bitů (bajt). Morseova abeceda používá k úpravě textu napsaného v běžném jazyce tři symboly (tečku, čárku a mezeru, která se často zapisuje pomocí lomítka) a původně sloužila k tomu, aby mohl být text předán pomocí telegrafu. Kdokoliv dokáže na základě informace, že jde o ASCII kód nebo Morseovu abecedu, převést text zpět do otevřeného tvaru. Pokud by odesílatel a příjemce byli např. domluveni, že zamění použití čárek a teček v Morseově kódu (tedy již např. znak „.“ nebude vyjadřovat písmeno *e*, ale písmeno *t*), pak se jedná o šifru. Přesněji půjde o **jednoduchou záměnu**, kde **šifrová abeceda** jsou znaky Morseovy abecedy a **klíč** je záměna znaku šifrové abecedy tečky za čárku. Pokud bychom text ponechali v Morseově kódu, ale k jeho předání bychom např. použili obrázek, kde bude namalovaná různě dlouhá tráva (krátká tráva tečka, dlouhá čárka) půjde o steganografické utajení přenosu této zprávy. U velmi jednoduchých metod a šifrových systémů se rozdíl mezi kódem a šifrováním může zdát velmi malý, ale u opravdových šifrových systémů je naprosto zřetelný. Jakousi jednoduchou pomůckou (byť ne úplně přesnou) pro rychlé rozlišení může být, že šifrový systém používá k dešifrování zprávy klíč, který je znám pouze příjemci, zatímco při kódování se takovýto klíč nepoužívá. Rozlišujeme tedy mezi kódem a šifrou a kódováním a šifrováním.

Kód v kryptologii

V kryptologii má slovo kód také své místo. Vztahuje se k jednomu speciálnímu šifrovému systému, který pracuje s lingvistickými (jazykovými) prvky. Těmito prvky mohou být vybraná slova, celé věty nebo souvětí. Např. kód *vejce* může znamenat granát, kód *oko* může znamenat *chci se s tebou sejít* apod. Pokud je význam kódů veřejně známý (např. radiový Q-kód, kde QRX znamená *zavolám později*, QTC *mám pro vás telegram*), jedná se o kód v klasickém smyslu. Pokud je význam kódů utajen, jedná se o speciální šifrový systém, který se nazývá **kódová kniha** nebo v případě, kdy není seznam kódů příliš obsáhlý, **kódová** nebo **signální tabulka**. Kódy jsou výhodné pro situace, se kterými se počítá při jejich přípravě, a proto obsahují kódové ekvivalenty jen pro vybrané otevřené texty, šifry se hodí pro jakékoliv situace, neboť umí převést do šifrového tvaru libovolný otevřený text.