Técnicas Criptográficas

MiEI, MiEBM

Óscar Pereira

oscar@di.uminho.pt

Uminho, EEng, DI (Gualtar)

1º semestre – 2020/21

Criptografia

- `kryptós + graphein` = `oculto + escrita`
- Variante: ***Criptologia***
- `kryptós + logia` = `oculto + estudo`

E falando em coisas ocultas...

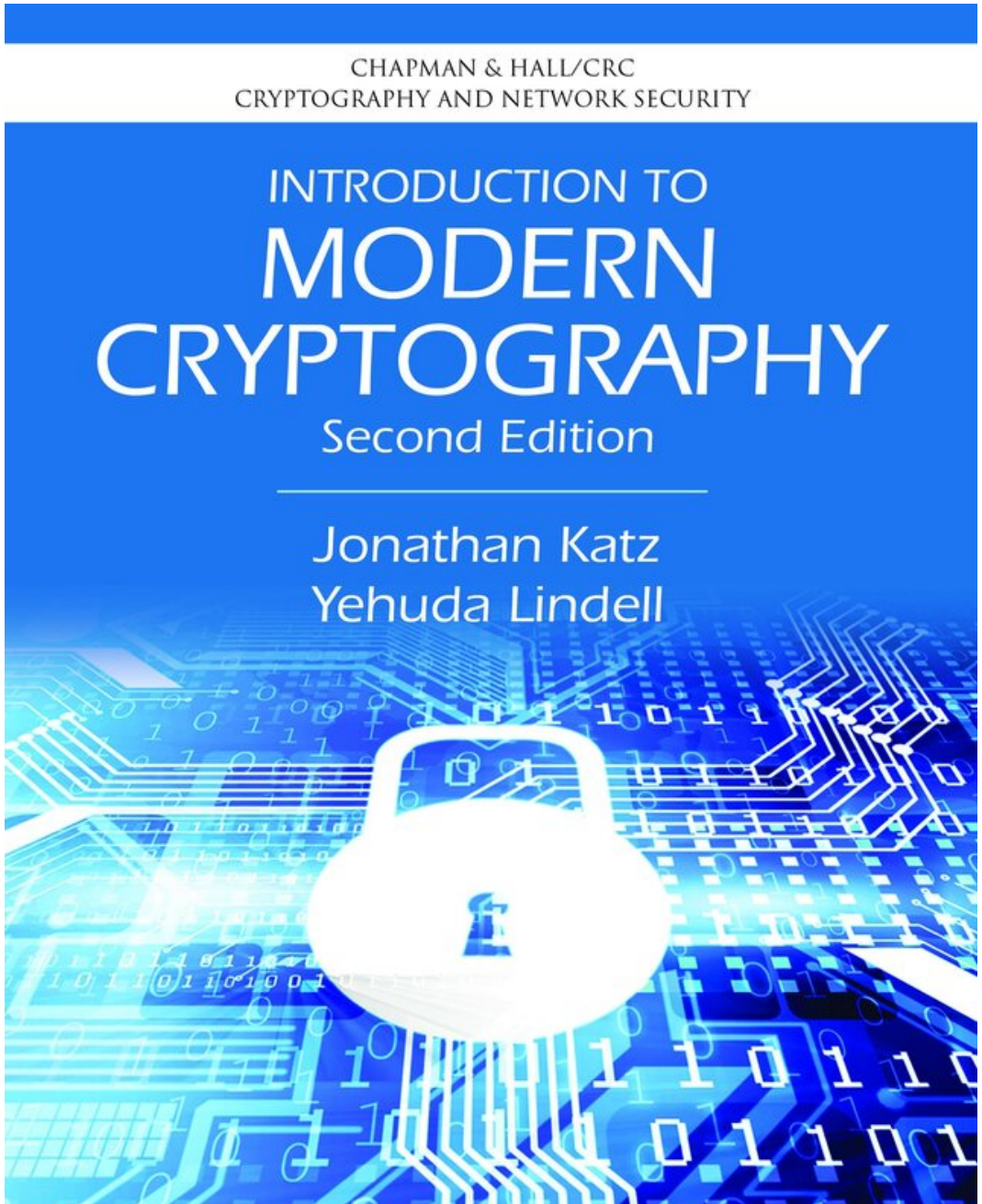
Perl!

While many languages can be used to encrypt data, PERL has something built-in that gives you encryption.

PERL calls it "syntax".

`https://uncyclopedia.ca/wiki/Perl`

O livro a seguir



Conteúdo lectivo

- Terminologia e Conceitos criptográficos
- Criptografia simétrica; assimétrica; PKI
- Frameworks e Bibliotecas criptográficas na codificação de sistemas seguros
- Certificação e Infra-estruturas de chave pública (X.509)
- Proteção de redes e Protocolos relevantes (e.g. IPSec; HTTPS; SSH,...)

Um pouco de história...

Communication Theory of Secrecy Systems (1949)

Claude E. Shannon (1916–2001)

Três tipos de “confidencialidade” (Shannon, *op. cit.*)

- Esconder a existência da mensagem secreta (e.g. tinta invisível)
- Maquinaria “especial” (e.g. inversão de aúdio)
- **Confidencialidade “algorítmica” (cifras, códigos, etc.)**

Alguma terminologia

- Texto limpo (plaintext), (de)cifragem, criptograma (ciphertext)
- `Gen`, `Enc`, `Dec`
- "Keyed function"

Criptografia *A.C.*—"Antes dos Computadores"

Cifras Clássicas: no alfabeto `ABCDEF`

- ***Cifra de César***: não há chave; a cifra ***é*** a chave!
- ***"Shift cipher"***: rotação arbitrária. Há 6 chaves.
- Substituição ***mono-alfabética***: permutações aleatórias. Há $6!$ chaves.
- Substituição ***poli-alfabética***: chave é sequência finita de permutações aleatórias.
  $\rightarrow$ Para sequência com m permutações, há $(6!)^m$ chaves.
- Exemplo (simplificado): cifra de Vigenère. Chave é sequência aleatória de *rotações*. Há 6^m chaves.
- Exemplo de sequência de permutações aleatórias... alguém conhece?

Criptografia *A.C.*—"Antes dos Computadores"

Cifras: por blocos ou sequenciais ("stream ciphers")

- O último caso acima (sub. poli-alfabética) é uma cifra sequencial
- Vulnerável na mesma a um ataque por frequências...
- Solução: permutar ***blocos de caracteres***.

Cifra de Vernam (circa 1917)

- Como contornar o ataque à cifra de Vigenère?
  - Estendendo a chave até ter o mesmo comprimento da mensagem: OTP!
- Distância de unicidade (ver Shannon, *Secrecy*, §14, §15)

Segurança Perfeita: ver Katz e Lindell, cap. 2.

Segurança Perfeita

Cifra de Vernam (circa 1917)—mensagem pode ser repudiada:

Plain	heilhitler
Key	wclnbtdefj
Cipher	DGTYIBWPJA

Ver Ross Anderson, *Security Engineering*, cap. 5.

Segurança Perfeita

Cifra de Vernam (circa 1917)—mensagem pode ser repudiada:

Plain	hanghitler
Key	wggsbtdefj
Cipher	DGTYIBWPJA

Ver Ross Anderson, *Security Engineering*, cap. 5.

Chave privada vs. chave pública

Indagação...

Haverá vida (criptográfica) para lá da confidencialidade?

Prática!

https://cryptography.io/

Obrigado pela atenção!

Dúvidas