Addenda et Corrigenda per "Manuale di Crittografia" Ulrico Hoepli Editore, Milano (2015)

Alessandro Languasco & Alessandro Zaccagnini

29 febbraio 2020

1 Correzioni inserite nella prima ristampa (maggio 2016)

Si ringrazia Enrico Sintoni per averci segnalato alcuni degli errori e/o precisazioni sottostanti. Se il numero della riga è negativo si intende che deve essere contata dal basso.

Pag.	riga.	Errata	Corrige
79.	-11.	$x \in \mathbb{Z}_p^*$	$x \in \mathbb{Z}_{p-1}$
101.	7.	$r = (10)_2 = 3$	$r = (10)_2 = 2$
123.	-11.	variante	varianti
129.	-8.	otteniamo che ...	si ha che ...
129.	-8.	Pertanto $r \nmid n$ e quindi ...	Pertanto $r \nmid n$ e $r \nmid \Pi$; quindi ...
133.	16.	$\mathcal{O}\big(N^{1/2}(\log N)^3\big)$	$\mathcal{O}\big(N^{1/2}(\log N)^2\big)$
133.	-8.	$\le f(N)/(\log N)^3$	$\le f(N)/(\log N)^2$
167.	10.	$\frac{i_k - i_h}{d} \equiv \frac{j_h - j_k}{d} \bmod \frac{m}{d}$	$y\frac{i_k - i_h}{d} \equiv \frac{j_h - j_k}{d} \bmod \frac{m}{d}$
167.	12.	$j_h - j_k \equiv i_k - i_h \bmod m$	$j_h - j_k \equiv y(i_k - i_h) \bmod m$

2 Ulteriori correzioni (01/02/2017)

- ulteriori errori di stampa

Pag.	riga.	Errata	Corrige
35.	-4.	... EDE?	... EDE.
138.	-5.	... di $N^{1/2}$ iterazioni,	... di circa $N^{1/2}$ calcoli di massimo comun divisore,
139.	1.	Nella figura 5.3	va scambiato 40 con 54
139.	17.	$(5 - 40, 91) = 7$	$(5 - 54, 91) = 7$

- Ringraziamo Ottavio G. Rizzo per la segnalazione seguente (26/10/2016).

  A pagina 183 del testo i punti 1) e 2) del paragrafo intitolato "One time password" sono formulati in maniera imprecisa; si consiglia di sostituirli con i seguenti:

  1) la combinazione di quanto viene visualizzato sul token e dei codici personali rilasciati dalla banca, o decisi dall'utente al momento della stipula del contratto, è unica, ossia non vi è un altro utente che allo stesso momento possa utilizzare la medesima combinazione di codici personali-codice del token;
  2) quanto viene visualizzato sul token ha bassa probabilità di essere ripetuto (da qui il nome di One Time Password); ossia si è in genere in presenza di un generatore pseudocasuale di numeri avente un periodo sufficientemente grande in modo da assicurare una ragionevole probabilità di non ottenere una ripetizione del codice generato dal token nel periodo totale di tempo di utilizzazione del token stesso.

3 Addenda

3.1 Pseudoprimi forti

Ricordando la notazione del §11.8.3 di [4], denotiamo come ψ_k il più piccolo intero composto tale che è uno pseudoprimo forte per le prime k basi prime. Recentemente Sorenson and Webster [7] hanno mostrato che

$$\psi_{12} = 318665857834031151167461 = 399165290221 \cdot 798330580441$$

$$\psi_{13} = 3317044064679887385961981 = 2 \cdot 5 \cdot 1287836182261 \cdot 2575672364521$$

estendendo in tal modo i precedenti risultati.

3.2 Ancora sui numeri di Carmichael

Recentemente è apparso un articolo di Bach e Fernando [1] in cui si fanno ulteriori osservazioni riguardanti gli algoritmi di pseudoprimalità ed i numeri di Carmichael.

3.3 Fattorizzazione di numeri RSA-challenge

Il 13 maggio 2016 è stata realizzata la fattorizzazione di RSA-220, un numero di 220 cifre decimali appartenente alla lista degli *RSA-challenges*, da parte di S. Bai, P. Gaudry, A. Kruppa, E. Thomé e P. Zimmermann, si veda [6]. Per completezza riportiamo che

```
RSA220 = 22601385262034057849416540486101975135080389157197767183211977681094456418179666766085931213065825772506315628866769704480700018111497118630021124879281994874820660701310665866460833279828035603792053919801399464969552611
```

e che i suoi due fattori primi sono

```
p = 6863656412267566274382371499288437800130842239979164844621244993321541061441464266793821364420840201920549990687
```

```
q = 3292907439486349812049301549212935291916455196536233952462686051169290349309465246333782486639073819176571260 3
```

Il 2 Dicembre 2019, è stata realizzata la fattorizzazione di RSA-240, un numero di 240 cifre decimali appartenente alla lista degli *RSA-challenges*, da parte di F. Boudot, P. Gaudry, N. Heninger, E. Thomé and P. Zimmermann, si veda [3]. Per completezza riportiamo che

```
RSA240 = 124620366781718784065835044608106590434820374651678805754818788832896668011882108550360395702725087475098647684384586210548655379702539305718912176843182863628469484053016144164304680668756994152469931857041830305125495943713721590292360991
```

e che i suoi due fattori primi sono

```
p =  5094359522858399145550510235808437141326483820241114731866602965218212064697467006203164434788738376062523720496193345 17
```

```
q = 2446242088383181505678131390240028966538020925789314014520412213365584770951781552582188977350305906690413020459080714 47
```

Il 28 Febbraio 2020, è stata realizzata la fattorizzazione di RSA-250, un numero di 250 cifre decimali appartenente alla lista degli *RSA-challenges*, da parte di F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann, si veda [2]. Per completezza riportiamo che

```
RSA-250 = 2140324650240744961264423072839333563008614715144755017797754920881418023447140136643345519095804679610992851872470914587687396261921557363047454770520805119056493106687691590019759405693457452230589325976697471681738069364894699871578494975937497937
```

e che i suoi due fattori primi sono

```
p = 641352894770715802787901901705773890848250147429434472081168596320245323446302386
235987526683477087376619255856946397988533 67
```

```
q = 333720275949781565562260106053551142279407603447675546667845209870238417292100370 8
025744867329688187756571898625803693206271 1
```

3.4 Analisi degli algoritmi di fattorizzazione

Una interessante panoramica della possibilità di avere algoritmi di fattorizzazione particolarmente efficienti in dipendenza della conoscenza di uno tra $\varphi(N)$, $\lambda(N)$ e l'ordine di elementi in $\mathbb{Z}_N^*$ si trova nell'articolo di Morain, Renault e Smith [5].

References

[1] E. Bach and R. Fernando, *Infinitely many carmichael numbers for a modified miller-rabin prime test*, Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC 2016, ACM, 2016, pp. 47–54.

[2] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, *Factorization of RSA-250*, 2020, `https://caramba.loria.fr/rsa250.txt`.

[3] F. Boudot, P. Gaudry, N. Heninger, E. Thomé, and P. Zimmermann, *Factorisation of RSA-240 with CADO-NFS*, 2019, `https://caramba.inria.fr/dlp240-rsa240.txt`.

[4] A. Languasco and A. Zaccagnini, *Manuale di Crittografia*, Ulrico Hoepli Editore, 2015, `http://www.hoepli.it/libro/manuale-di-crittografia/9788820366902.html`.

[5] F. Morain, G. Renault, and B. Smith, *Deterministic factoring with oracles*, arXiv.org (2018), `https://arxiv.org/abs/1802.08444`.

[6] B. Shi, P. Gaudy, A. Kruppa, E. Thomé, and P. Zimmermann, *Factorisation of RSA-220 with CADO-NFS*, 2016, `https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2016-May/000626.html`; `https://members.loria.fr/PZimmermann/papers/rsa220.pdf`.

[7] J. P. Sorenson and J. Webster, *Strong Pseudoprimes to Twelve Prime Bases*, Math. Comp. (2017), no. 86, 985–1003, `http://dx.doi.org/10.1090/mcom/3134`.