
# La bacchetta magica non esiste

## Osservazioni alla Risoluzione del Consiglio dell'Unione Europea

***Security through encryption***
***and***
***security despite encryption***

**DRAFT PER DISCUSSIONE APERTA**

**16 dicembre 2020**

Iniziativa Nazionale De Componendis Cifris
www.decifris.it

# Premessa

Il Consiglio dell'Unione Europea ha discusso a lungo una Risoluzione intitolata ***Security through encryption and security despite encryption***, la cui versione finale si trova al link

eu-council-encryption-declaration-13084-20-rev1.pdf (statewatch.org)

Tale risoluzione è stata approvata ufficialmente il 14 dicembre 2020

Crittografia: il Consiglio adotta la risoluzione "La sicurezza attraverso la crittografia e nonostante la crittografia" - Consilium (europa.eu)

La **comunità crittografica europea** è molto critica di questa Risoluzione e sta organizzando una petizione online di forte protesta, reperibile a questo link:

https://sites.google.com/view/scientists4crypto/start

La **comunità crittografica italiana**, raccolta nell'iniziativa **De Componendis Cifris**, condivide in gran parte la protesta dei colleghi europei.

In questa prima versione del documento spieghiamo le nostre ragioni.
Auspichiamo commenti e integrazioni da parte della community crittografica.

Auspichiamo anche un'interazione con altre comunità scientifiche che si interessano di tematiche affini alla Crittografia.

# Stesura di questo documento

**Coordinatore**

Prof. Massimiliano Sala, professore ordinario presso l'Università degli Studi di Trento, Dipartimento di Matematica, **Acting Director** di **De Componendis Cifris**

**Contributi**

Hanno contribuito:

- Prof. Marco Baldi, professore associato presso l'Università Politecnica delle Marche, Dipartimento di Ingegneria dell'Informazione, coordinatore del gruppo tematico **PQCifris** (gruppo sui cifrari post-quantum)
- Prof. Norberto Gavioli, professore associato presso l'Università degli Studi dell'Aquila, Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica, coordinatore del gruppo tematico **MathCifris** (gruppo sugli aspetti matematici della Crittografia)
- Prof. Massimo Giulietti, professore ordinario e direttore del Dipartimento di Matematica e Informatica presso l'Università degli Studi di Perugia, coordinatore degli **Stage e Tirocini** della De Componendis Cifris
- Prof. Roberto La Scala, professore associato presso l'Università degli Studi di Bari, Dipartimento di Matematica, coordinatore dei seminari locali della **De Componendis Cifris**
- Prof. Marco Pedicini, professore associato presso l'Università degli Studi di Roma Tre, DIpartimento di Matematica e Fisica, coordinatore del gruppo tematico **CifrisCloud** (gruppo sulla Cloud Encryption)
- Prof. Silvio Ranise, Head of Security & Trust Unit, Fondazione Bruno Kessler, organizzatore dei seminari locali **De Cifris Athesis**
- Prof. Andrea Visconti, ricercatore presso l'Università degli Studi di Milano, Dipartimento di Informatical, coordinatore delle **CryptoWars**
- Prof. Ivan Visconti, professore ordinario presso l'Università degli Studi di Salerno, Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica applicata, coordinatore del gruppo tematico **CifrisChain** (gruppo Blockchain)

# Disamina della Risoluzione

Il titolo della Risoluzione riassume molto bene il suo contenuto "***Security through encryption and security despite encryption"***, cioè la tesi che si possa certamente ottenere sicurezza tramite la crittografia, ma la si possa ottenere anche nonostante sia usata la crittografia.

Nel dettaglio del documento troviamo:

- il **preambolo**,
  in cui si espongono principi generali e certamente condivisibili come ad esempio
  " *Encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society*."
  e
  "*At the same time, the European Union needs to ensure the ability of competent authorities in the area of security and criminal justice*,"

- un capitolo su **Current use/state of encryption,**
  dove si riassumono gli usi della Crittografia, con una visione molto positiva della stessa, come ad esempio
  "*It is a means to protect individuals, civil society, critical infrastructures, media and journalists, industry and governments by ensuring the privacy, confidentiality, data integrity and availability of communications and personal data: it is evident that all parties benefit from encryption technology*."
  e
  "*This is positively reflected in an increasing response by the communication and application industry, where the majority of instant messaging apps and other online platforms have also implemented end-to-end encryption*."

- un capitolo su Challenges for ensuring security,
  dove iniziano ad apparire frasi meno condivisibili, come questa
  "*Independently of the technological environment of the day, it is therefore essential to preserve the powers of competent authorities in the area of security and criminal justice through lawful access to carry out their tasks, as prescribed and authorised by law*"

- un capitolo su **Striking a right balance,**
  in cui si cerca un difficile compromesso tra esigenze conflittuali con frasi come
  *"The European Union continues to support strong encryption."*
  *che contrasta con "upholding the possibility for competent authorities in the area of security and criminal justice to lawfully access relevant (encrypted n.d.r) data for legitimate, clearly defined purposes in fighting serious and/or organized crimes and terrorism, including in the digital world".*

- un capitolo su **Joining forces with the tech industry,**
  in cui gli estensori della Risoluzione si rendono conto che le due loro richieste conflittuali non hanno valide soluzioni unanimemente accettate dalla comunità scientifica e sperano in qualche imprevedibile compromesso tecnologico:
  *"The European Union strives to establish an active discussion with the technology industry, while associating research and academia, to ensure the continued implementation and use of strong encryption technology. Competent authorities must be able to access data in a lawful and targeted manner .., while upholding cybersecurity".*

- un capitolo su **Regulatory framework**,
  che si sofferma sullo schema normativo, con ancora una volta frasi che riteniamo poco realistiche, come
  *"Potential technical solutions will have to enable authorities to use their investigative powers .. while respecting common European values and upholding fundamental rights and preserving the advantages of encryption".*

- Un capitolo finale su **Innovative investigative capabilities,**
  che sostanzialmente ribadisce la fiducia nella capacità tecnologica di risolvere il conundrum, come ad esempio
  *"Technical and operational solutions anchored in a regulatory framework built on the principles of legality, necessity and proportionality should be developed ,,,, although there should be no single prescribed technical solution to provide access to encrypted data".*

# La nostra opinione scientifica

Noi abbiamo dedicato la nostra intera vita lavorativa allo studio della Crittografia, chi da un punto di vista teorico, chi da un punto di vista applicativo/implementativo.
La Crittografia è un campo molto ampio, che comprende primitive crittografiche, funzioni avanzate, protocolli, etc.
Limitandoci per semplicità agli algoritmi di cifratura, riteniamo in coscienza e nel pieno della nostra competenza professionale che le seguenti quattro frasi siano vere:

1. ci sono solo due metodi per permettere accesso privilegiato al dato cifrato: introdurre vulnerabilità nell'algoritmo di cifratura dei dati o in quello di generazione delle chiavi;

2. se uno schema di cifratura viene creato con una debolezza intrinseca, pur nota solo ai progettisti, allora si tratta di uno schema debole e sicuramente qualche vulnerabilità verrà trovata e sfruttata;

3. se le chiavi di cifratura vengono create con meccanismi che a utenti privilegiati permettono di dedurle (o dedurne altre equivalenti), quindi violando il principio di randomicità delle stesse, allora gli attaccanti riusciranno a trovare il modo di fare altrettanto, non necessariamente quello previsto dai progettista ma altrettanto letale;

4. se uno schema di cifratura prevede un ente privilegiato con una chiave speciale, allora questo ente sarà costantemente attaccato e il rischio che la chiave speciale venga compromessa sarà molto alto.

Così come non si proibisce la produzione di guanti anche se questi possono essere usati dai criminali per nascondere le proprie impronte, riteniamo sia controproducente perseguire la strada di progettare cifrari/protocolli crittografici in modo da permettere accesso privilegiato a certi attori, come le Forze dell'Ordine.

Anche a noi piacerebbe che, ad esempio, le prove dei crimini e i messaggi dei terroristi fossero decrittabili da chi legittimamente opera nel contrastare le minacce della nostra società, ma questo non è possibile farlo a meno di non lasciare i cittadini, le aziende e la Pubblica Amministrazione privi di difese crittografiche.

**Iniziativa Nazionale De Componendis Cifris**
**www.decifris.it**


Inoltre, nessuno può costringere i criminali a usare la Crittografia imposta dalle leggi: loro, quando utile ai loro fini, possono continuare ad usare gli algoritmi sicuri usati fino ad oggi, oppure possono agevolmente procurarsi nuovi algoritmi, e.g. nel Dark Web.

Quindi si rischierebbe di arrivare al paradosso in cui:

- i cittadini e le aziende, che operano lecitamente, si troverebbero con crittografia debole, in balia dei cyber criminali,
- mentre chi opera illecitamente rimane al sicuro, potendo usare crittografia forte.

Riformulando un'ultima volta quanto detto finora, possiamo dire che non è realistico pensare che la legge riesca a ostacolare l'uso della crittografia forte per usi illeciti. D'altro canto, una crittografia debole può minare la sicurezza di impianti industriali, di riserve energetiche, del normale funzionamento degli apparati amministrativi, fino a mettere in ginocchio anche grandi organizzazioni, oppure (potenzialmente) falsare l'esito di votazioni. Senza dimenticare la violazione della confidenzialità delle comunicazioni dei cittadini.
Usare una crittografia forte "per legge" vuol dire combattere la criminalità ad armi pari, l'alternativa è invece darle un vantaggio.

La nostra conclusione è che **security despite cryptography** sia solo un'utopia, e chiediamo pertanto che la Risoluzione sia al più presto ritirata.

Vogliamo concludere questo documento con la seguente precisazione.
Una crittografia forte è necessaria per la sicurezza, ma non sufficiente. Molto dipende da come gli algoritmi vengono usati. Le situazioni possono variare molto, in base all'ambiente di esecuzione, l'interazione con dispositivi di rete, le interfacce software e hardware, etc. Una valutazione globale della protezione delle informazioni va chiaramente oltre la crittografia.