BRUNO OLIVEIRA GUIMARÃES DINIZ

O PROCESSO DE INOVAÇÃO NO DOMÍNIO DA INFORMAÇÃO: O CASO DA CRIPTOGRAFIA

Monografia apresentada como requisito obrigatório para aprovação no Curso de Ciências Econômicas da Universidade Federal do Paraná.

Orientador: Prof. José Wladimir Freitas da Fonseca

Curitiba

2013

TERMO DE APROVAÇÃO

BRUNO OLIVEIRA GUIMARÃES DINIZ

O PROCESSO DE INOVAÇÃO NO DOMÍNIO DA INFORMAÇÃO: O CASO DA CRIPTOGRAFIA

Monografia aprovada como requisito parcial para obtenção do grau de Bacharel no Curso de Graduação em Ciências Econômicas, Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná, pela seguinte banca examinadora:

Orientador: Prof. José Wladimir Freitas da Fonseca
Departamento de Ciências Econômicas, UFPR

Prof. Mariano de Matos Macedo
Departamento de Ciências Econômicas, UFPR

Prof. Gustavo Pereira da Silva
Departamento de Ciências Econômicas, UFPR

Curitiba, 21 de Março de 2013

RESUMO

O objetivo do presente trabalhofoianalisar a importância e a evolução do processo de inovação no domínio da informação. A fim de concluir sobre a importância da inovação nesse processo foi apresentado todo um arcabouço teórico com base na Teoria da Inovação Evolucionista, destacando principalmente as condicionantes da inovação e suas implicações na sociedade. Além disso, fez-se uma análise da história da criptografia, que foi utilizada como estudo de caso para comprovação empírica das teses apresentadas na Teoria. Tomando como base o presente referencial teórico e o estudo de caso apresentado, elaborou-se uma conclusão condizente e factível ao final.

Palavras-chave: Inovação; Teoria Evolucionista da Inovação; Criptografia; Domínio da Informação; Tecnologia.

ABSTRACT

The main goal of the present project was to evaluate the importance and evolution of the innovation process related to information. With the purpose to conclude about the importance of innovation in this process, the Evolutionary Innovation Theory was used pointing out the constraints of innovation and its implications towards the society. Besides that, an analysis was made based on the history of cryptography that was used to prove the applicability of the theses as an empirical basis.

Keywords: Innovation; Evolutionary Innovation Theory; Cryptography; Technology

SUMÁRIO

1 INTRODUÇÃO

A economia passa por um momento onde o conhecimento e agilidade desempenham papeis fundamentais em seus processos. O desempenho dos agentes (empresas, indivíduos e entidades públicas) está intimamente relacionado ao nível de conhecimento que cada um deles os detém. E dentro desse ambiente, a inovação possui papel central, e isso já ficou claro para governos e empresas, vide os altos investimentos estimulando Ciência e Tecnologia (no caso dos governos) e Pesquisa e Desenvolvimento (no caso das empresas).

Como bem define Schumpeter[1]: "inovações radicais provocam grandes mudanças no mundo, enquanto inovações incrementais preenchem continuamente o processo de mudança". Devido ao fato de que o conhecimento proveniente de uma inovação não ser replicado instantaneamente por nenhum outro agente, as inovações são capazes de prover vantagens aos que são detentores das mesmas, por período de tempo suficiente até que seus concorrentes se desenvolvam e alcancem o mesmo estágio de conhecimento.

Em relação à agilidade, podemos apresentar a Internet como maior expoente da necessidade dela nos dias atuais. A Internet vem mudando a forma com que nos comunicamos, alterando a rotina de pessoas e empresas, que hoje não precisam mais ir a bancos para efetuarem pagamentos ou transferências bancárias, ou irem a lojas para efetuarem compras.

Um número que reflete essa alteração no hábito das pessoas, especificamente no Brasil, é o número de transações bancárias realizadas pelo Internet Banking. Em 2011 o crescimento das operações pela Internet cresceram 19,8%, o que representou 15,7 bilhões de transações[2].

Com o aumento das operações e do uso da Internet, surge a necessidade também de sistemas de segurança com a finalidade de garantir a operacionalização e o sigilo de diversas dessas operações, e o sistema que atualmente é utilizado e adequado para prover essa segurança é o da criptografia de rede, que se resume a uma combinação de números primos que formam chaves que para serem decifradas

---

[1] SCHUMPETER, J. (1934). *The Theory of Economic Development,* Harvard University Press, Cambridge, Massachusetts

[2] BOUÇAS, C. FEBRABAN: Internet Banking vai superar transações de autoatendimento. **Valor Econômico**. Disponível em: <http://www.valor.com.br/empresas/2721580/febraban-internet-banking-vai-superar-transacoes-de-autoatendimento>. Acesso em: 13/03/2013

demandam alta capacidade técnica e de processamento, tempo e sorte por parte daqueles que desejam acessar os dados.

Dada a importância do tema na atualidade, esse estudo tem como objetivo elaborar uma análise sobre a criptografia, processo que ao longo dos anos já sofreu tanto inovações radicais, quanto inovações incrementais, e hoje desempenha papel fundamental no intuito de oferecer segurança e sigilo aos sistemas de rede. Utilizaremos a Teoria Evolucionista da Evolução para analisar de que forma ocorre esse processo.

Assim sendo, este trabalho está dividido em três seções. Na primeira seção faz-se uma análise da Teoria da Inovação, com ênfase na Teoria Evolucionista. Na segunda parte analisa-se o processo histórico de desenvolvimento da criptografia. A terceira seção dedica-se avaliar e identificar relações entre o desenvolvimento da criptografia com a Teoria da Inovação Evolucionista. Por fim, sumaria-se as principais conclusões.

2 TEORIA EVOLUCIONISTA DA INOVAÇÃO

A Teoria da Inovação Tecnológica teve seu início com Joseph Alois Schumpeter, que foi o primeiro teórico a identificar que a importância de incorporar a questão da troca industrial e da inovação dentro do campo da análise econômica. Schumpeter sem dúvidas abriu caminho ao tomar em consideração a mudança tecnológica dentro da economia neoclássica, porém, seu modelo possuía alguns problemas que limitam algumas análises (p.e. analisa ciência e técnica de forma separada dentro de um processo de inovação). Por isso, neste trabalho, utilizamos a Teoria Evolucionista da Inovação, que teve suas bases extraídas da Teoria da Inovação Schumpeteriana, porém foi atualizada e aperfeiçoada pelos autores evolucionistas.

A Teoria Evolucionista da Inovação neste trabalho será estudada a partir das obras de Richard R. Nelson e Sidney G. Winter, *AnEvolutionaryTheoryofEconomicChange*, e de G. Dosi, *TechnicalChange and Industrial Transformation*.

Os neoschumpeterianos, como também são conhecidos os economistas que desenvolvem a Teoria Evolucionista, concebe o desenvolvimento tecnológico como um processo evolutivo, dinâmico, acumulativo e sistêmico, onde para sua

compreensão se faz necessária à integração entre a dinâmica econômica e a dinâmica do desenvolvimento tecnológico.

Para NELSON E WINTER (1982, p. 206), as ideias-chave da Teoria Evolucionista são:

> A qualquer momento as firmas são vistas como possuidoras de várias aptidões, procedimentos e regras de decisão determinando o que elas fazem diante das condições externas. Elas também se envolvem em várias operações de "busca", por meio das quais descobrem, julgam e avaliam mudanças possíveis de suas maneiras de fazer as coisas. As firmas cujas decisões são lucrativas, dentro do ambiente de mercado, conseguem expandir-se; as que não são lucrativas se contraem. O ambiente de mercado que circunda as firmas individuais pode ser parcialmente endógeno ao sistema de comportamento tomado como um todo, por exemplo, os preços dos produtos e dos fatores que podem ser influenciados pela oferta de produtos do ramo e pela demanda dos insumos.

A Teoria Evolucionista apresentada por Nelson e Winter apresenta muitas semelhanças com a Teoria de mesmo nome apresentada por Darwin e Lamarck no século XIX, principalmente porque em ambas a variação é estocástica e a seleção não é determinista. Porém, as diferenças entre a teoria econômica e a biológica são fundamentais no contexto da inovação. Para Nelson e Winter não há conceito de equilíbrio. Para os autores, as variações são pequenas, mas não são aleatórias e fazem parte de um processo de busca. Por fim, as empresas não podem reproduzir-se, apenas diminuir ou aumentar de tamanho.

Estas diferenças permitem fundamentar algumas ideias que surgiram com Schumpeter e que foram reafirmadas por Nelson e Winter, em particular a de que a competência é um processo e não um estado que, portanto, existem ganhadores e perdedores. Além dessa, a ideia de que existe um trade-off entre eficiência estática associada a competência geral e a eficiência dinâmica da competência restringida.

Quando analisa-se a mudança técnica, NELSON E WINTER (1982, p. 210), afirmam que:

> "...as atividades de P&D das firmas são modeladas em relação à distribuição de probabilidade do surgimento de novas técnicas diferentes. Mas, alternativamente, pode ser discutida em termos de uma distribuição de coisas que uma firma poderia "criar". Em qualquer um dos casos, a distribuição poderia ser em função do tempo (as oportunidades poderiam evoluir com o tempo), da política de P&D da firma (algumas firmas podem gastar mais ou executar tipos de P&D diferentes de outras), da técnica existente na firma (a pesquisa pode ser extremamente local) e de outras variáveis."

De outra maneira, DOSI (1988) construiu o que se chama de "modelo estrutural débil" no qual o comportamento e estratégia das empresas aparecem determinados por condições estruturais que definem quais os graus de liberdade que a empresa possui para agir. Por esse sistema, ou autor busca unir duas abordagens que até então eram tidas como dicotômicas: a abordagem microeconômica do comportamento inovador e a dinâmica do sistema em seu conjunto.

Através da análise dos resultados de pesquisas empíricas, Dosi concluiu que os inputs científicos jogam um papel crescente no processo de inovação e as atividades de P&D apresentam uma crescente complexidade que faz com que o processo de inovação seja algo planificado para o longo prazo dentro das empresas e levanta a hipótese de que a inovação seja uma resposta dos produtores frente as questões de mercado.

Nesse mesmo estudo, Dosi distingue três grandes sistemas: o científico, o tecnológico e o econômico, onde o foco principal foi o sistema tecnológico e suas interfaces com as variáveis econômicas.

DOSI (2006, p.40) inicia seu raciocínio, definindo tecnologia da seguinte maneira:

> "Definimos a tecnologia como um conjunto de parcelas de conhecimento – tanto diretamente "prático" (relacionado a problemas e dispositivos concretos), como "teórico" (mas praticamente aplicável, embora não necessariamente já aplicado) – de know-how, métodos, procedimentos, experiências de sucessos e insucessos e também, é claro, dispositivos físicos e equipamentos. Os dispositivos físicos existentes incorporam as realizações do desenvolvimento de uma tecnologia, de uma dada atividade de resolução de problemas".

Define também progresso técnico como processo sequencial de resolução de problemas no marco de um paradigma tecnológico, seguindo uma trajetória tecnológica.

Os conceitos centrais aqui são paradigma tecnológico e trajetória tecnológica. Define-se paradigma tecnológico "como um "modelo" e um "padrão" de solução de problemas tecnológicos selecionados, baseados em princípios selecionados, derivados das ciências naturais, e em tecnologias materiais selecionados" (DOSI, 2006, p. 41). Já a trajetória tecnológica aparece como a

solução que é dada para os paradigmas que são enfrentados, com foco na exploração de oportunidades tecnológicas.

Apesar de algumas diferenças, tanto para Dosi quanto para Nelson e Winter o meio ambiente econômico e social determina a trajetória que será seguida. O meio não modifica a trajetória nem as tecnologias que sobressairão umas sobre as outras, porém, discrimina e seleciona as que serão dominantes em diversos aspectos. Para eles o entorno determina a via através da qual o uso relativo das diferentes tecnologias muda com o tempo.

Nelson e Winter consideram principalmente elementos do mercado e extramercado para definirem o modelo geral de entrono de seleção. Para eles, a natureza dos benefícios e custos previstos pelas organizações que vão decidir a adotar ou não adotar uma inovação; a forma em que as regras e preferências do regulador e do consumidor influem no que é rentável; a relação entre benefício e expansão ou contração de unidades ou organizações particulares, além da natureza dos mecanismos pelos quais a organização aprende sobre as inovações bem sucedidas de outras organizações e os fatores que facilitam ou impedem a imitação.

Dosi analisa principalmente os fatores econômicos, institucionais e sociais que influenciam no processo de seleção, mas também analisa a influência que as mudanças no entorno exercem sobre a própria mudança técnica.DOSI (2006, p.53), cita que "as mudanças no meio ambiente econômico constituem uma característica permanente do sistema: frequentemente, essas mudanças estimulam o simples progresso técnico ao longo de uma trajetória tecnológica".

Ambos dão destaque especial para crescente influencia que os fatores extramercado possuem na decisão das empresas em inovar ou não. O papel principalmente do Estado e das forças político-institucionais em direcionar o desenvolvimento de tecnologias para determinadas áreas também é considerado no momento da inovação.

Além dessas, existem algumas características do processo de avanço tecnológico e das estruturas industriais que devem ser destacadas. São quatro as principais características de avanço tecnológico:

1. O caráter acumulativo e específico do progresso técnico;
2. As oportunidades tecnológicas que oferece cada paradigma tecnológico;
3. A apropriação privada dos efeitos da mudança técnica;

4. Incerteza dos resultados

A articulação dessas variáveis define qual será o regime tecnológico para um determinado período, que é a "combinação específica das bases de conhecimentos, fontes de oportunidades e possibilidades de apropriação".

As características específicas de cada indústria são fundamentais e influenciam diretamente na opção delas, quando tratadas individualmente na sua opção de ser uma firma inovadora ou não.

A respeito disso, Dosi também destacou outras variáveis que influenciam na determinação das firmas em desenvolverem ou não atividades inovadoras: Assimetrias tecnológicas – industrias de um mesmo setor podem estar em estágios diferentes de desenvolvimento tecnológico; Variedades tecnológicas – muitas vezes empresas com um mesmo grau de eficiência podem apresentar diferenças tecnológicas que podem impactar nas suas decisões de irem além na inovação ou não; Diversidade de comportamento – em cenários idênticos, as firmas podem apresentar atitudes diferentes em virtude da opção do próprio empresário; Diversidade organizacional – firmas possuem estruturas organizacionais diferentes umas das outras, o que implica maior ou menor especialização, e que consequentemente implica em maiores ou menores esforços em P&D.

Com este arcabouço teórico, que em suma diz que a inovação não se trata de um processo não aleatório, mas sim um processo dinâmico e de constante busca por soluções, onde o meio exerce influencia sobre de que forma e quais produtos as industrias devem inovar de acordo com suas capacidades frutos de um processo de acumulação de conhecimento, e também de estímulos ofertados por instituições públicas, no próximo capítulo será analisado o desenvolvimento histórico da criptografia sob a ótica evolucionista.

3 HISTÓRIA DA CRIPTOGRAFIA

Desde o início dos tempos o homem sente a necessidade de trocar informações uns com os outros, e da mesma forma que o ser humano sente a necessidade de se comunicar, este também sente a necessidade de guardar segredos, ocultar informações por motivos familiares, pessoais, religiosos ou governamentais. Qualquer que seja o motivo para se ocultar essas informações, com certeza existem outras pessoas querendo revela-las, dai surge a criptografia.

3.1 A CRIPTOGRAFIA ATÉ A II GUERRA MUNDIAL

Palavra com origem grega, cripto (kryptos) significa oculto, escondido e grafia (graphos) significa escrever. Essa é uma técnica muito antiga, e as primeiras mensagens criptografadas que se tem conhecimento datam de 1900 a.C.Khnumhotep era arquiteto do faraó Amenemhet II e construiu alguns monumentos que precisavam ser documentados, porém, essas informações não poderiam cair no domínio público. A alternativa encontrada foi trocar algumas palavras e trechos da escrita, caso essa caísse nas mãos de outras pessoas causaria confusão e essas não poderiam encontrar o que o faraó gostaria de manter em sigilo(KAHN, 1967).

Até a II Guerra Mundial, o sistema de criptologia utilizado era muito simplificado, era possível realiza-lo apenas com a escrita, por isso também ficou conhecido como criptografia manual, ou criptografia clássica. Nesse período, o avanço mais significativo que houve na tecnologia criptográfica foi à invenção da técnica de análise de frequência para quebrar cifras de substituição monoalfabética por Al-Kindi, que escreveu um livro sobre técnicas de criptoanálise, e análises de frequência.

Um bom exemplo de tecnologia criptografada desenvolvida nesse período foi o Código Morse. Desenvolvido pro Samuel Morse, FRANCO (2005) descreveu o código desenvolvido da seguinte maneira:

> "Originalmente, Morse imaginou numerar todas as palavras e em transmitir seus números através de telégrafo. O receptor, usando um enorme "dicionário", decifraria a mensagem onde as letras do alfabeto foram definidas pelo padrão "ponto e traço". Este novo código reconhecia quatro estados: voltagem-ligada longa (traço), voltagem-ligada curta (ponto), voltagem-desligada longa (espaço entre caracteres e palavras) e voltagem-desligada curta (espaço entre pontos e traços). Cada caractere (letras, números, sinais gráficos) possui seu próprio conjunto único de pontos e traços."

Nesse caso específico, além do código em si, outra vantagem é a possibilidade de transmitir a mensagem em longas distâncias.

Apesar de ter avançado no período até a II Guerra Mundial, em vista do ponto atual de evolução das mensagens criptografadas, esses avanços foram muito pequenos. Apenas a partir da utilização dessa técnica nos campos da II Guerrra

Mundial, principalmente pelos nazistas, é que houve uma grande evolução desta técnica (KAHN, 1967).

3.2 O DESENVOLVIMENTO DA CRIPTOGRAFIA NA II GUERRA MUNDIAL

Muitos métodos matemáticos foram desenvolvidos antes da II Guerra Mundial até 1932. Métodos esses que foram a base para o desenvolvimento do principal código desenvolvido nesse período pelo exército alemão, em 1928: O Enigma G.

O método consistia num teclado ligado a uma central codificadora composta por três discos rotadores. As posições dos rotadores definiam como cada letra seria codificada. Para entender quão grande foi o avanço com a implantação do Enigma G pelo exército alemão, se faz necessário entender exatamente como era o seu funcionamento, e FRANCO o resumiu da seguinte maneira:

> "O que tornava o código daEnigma tão difícil de quebrar era o enorme número de modos nos quais a máquina podiaser regulada. Em primeiro lugar, os três rotores na máquina eram escolhidos de uma seleçãode cinco que podia ser mudada e trocada para confundir os adversários. Em segundo lugar,cada rotor podia ser posicionado em 26 modos diferentes. Isto significava que a máquinapodia ser regulada em milhões de modos diferentes. E além das permutações permitidaspelos rotores, as conexões no quadro de chaveamento, na parte detrás da máquina, podiamser mudadas manualmente para fornecer um total de 150 trilhões de regulagens possíveis. Epara aumentar ainda mais a segurança, os três rotores mudavam de orientação continuamente, de modo que, cada vez que a letra era transmitida, a regulagem da máquina,e portanto o código, iria mudar de uma letra para outras. Assim se alguém digitasse"DODO" no teclado iria gerar a mensagem "FGTB", por exemplo – o "D" e o "O" eramtransmitidos duas vezes, mas codificados de modo diferente a cada vez."

Com certeza esse foi o avanço mais significativo até então na tentativa de ocultar informações de outros agentes (nesse caso, dos inimigos de guerra), porém, como todo método, esse também possuía falhas, e essas foram quebradas pela equipe chefiada pelo matemático inglês Alan Turing (fundador conceitual da computação moderna), que contou com o auxílio da Inteligência do exército francês para conseguir esse avanço fundamental para a vitória na II Guerra.

Os sistemas de criptografia utilizados até então, perderam sua eficácia face a utilização de computadores que podem facilmente decodificar suas cifras, porém, até meados do século XX foram extremamente eficazes em suas funções.

Apesar de decodificado, o Enigma G representou grande passo para atual estágio de segurança que os sistemas de criptografia possuem. Sem o desenvolvimento do método pelo exército alemão, e sem o alto empenho dos Aliados na tentativa de decodificar o sistema utilizado pelos nazistas, o sistema de criptografia de rede não teria sido idealizado e viabilizado pela grande potência militar que ascendeu da II Guerra Mundial (EUA), que desenvolveu os dois sistemas que avaliaremos a seguir e que são até hoje amplamente utilizados tanto na indústria bélica, quanto na indústria civil.

É importante observar que a passagem do sistema de criptografia do meio militar para o civil constitui por si só um spillover ou mesmo um spin-off do tipo tecnologia dual. Considerando a ampla temática que reveste o tema este trabalho deixa para futuras investigações a possibilidade de perceber a inovação e sua transferência de um ambiente para outro.

3.3 SISTEMAS DE CRIPTOGRAFIA DE REDE – ALGORÍTMO DES E RSA

A criptografia de rede tem sua maior vantagem em se utilizar de algoritmos para gerar seus códigos criptografados, fato esse que permite a geração de centenas de milhares de combinações, o que torna ainda mais difícil a tentativa de alguém em obter dados que o emissor desejar que sejam secretos[3]. Os principais métodos desenvolvidos e que serão analisados aqui são os algoritmos DES (criptografia simétrica) e os algoritmos RSA (criptografia assimétrica).

O algoritmo DES (Data EncryptionStandart) foi um avanço público (não-secreto), desenvolvido por pesquisadores da IBM, a convite do NationalInstituteof Standards and Technology (NIST) e do National Bureau of Standards, com a ajuda da National Security Agency (NSA). O envolvimento de tantos órgãos públicos e uma grande empresa de tecnologia demonstra a importância do projeto à época. O desenvolvimento desse sistema foi uma solicitação do governo norte-americano que desejava manter de forma sigilosa e segura informações confidencias, fundamentais para o sucesso do país na Guerra Fria.

Este algoritmo se utiliza de criptografia simétrica, ou seja, se utiliza de uma única chave secreta para ambos agentes da ação: o emissor e o receptor

---

[3]SINGH, S. (2004) - **O Livro dos Códigos**, Editora Record, São Paulo.

necessitam dessa chave antes do envio da mensagem. O poder de codificação geralmente costuma ser medido pelo tamanho da chave, como definiu FRANCO (2005): "geralmente as chaves de 40 bits são consideradas fracas e as de 128 bits ou mais, as mais fortes".

O DES é uma forma simples e segura de criptografar mensagens, porém, ainda assim apresentam falhas: Pelo fato de possuir uma única chave, necessita que antes do envio da mensagem ambos agentes a possuam, o que muitas vezes não pode ser armazenada de forma segura (STALLINGS, 2007). Além disso, não é possível identificar quem enviou a mensagem e, além disso, não permite a troca de informações de muitos usuários ao mesmo tempo.

Outra crítica que se fazia ao DES, mesmo poucos anos após a sua criação, é em relação ao tamanho da chave. Para uma série de especialistas, inclusive para os criadores da Criptografia de Chaves Públicas, Martim Hellman e WhitfieldDiffie, a chave desenvolvida era muito pequena, portanto, vulnerável a ataques de computadores com boa capacidade de processamento e com profissionais qualificados para a operação. Fato esse que foi comprovado anos mais tarde com dois ataques ao sistema, o primeiro em 1994, e o segundo que ficou conhecido como ataque de força bruta em 1998. Ataque esse que evidenciou a fragilidade do sistema para as finalidades do governo norte-americano que providenciou sua substituição o que acarretou no total desuso do sistema em 2004.

Mesmo com todos esses problemas, ainda nos dias atuais essa é uma forma bastante utilizada de criptografia (em casos onde o nível de segurança exigido não seja alto) e foi fundamental para o desenvolvimento de sua forma mais evoluída, o algoritmo RSA.

O algoritmo RSA[4] é conhecido como chaves assimétricas, ou chaves públicas, porque suas cifras podem ser reveladas a qualquer um em domínio público, porém, a mesma só poderá ser decifrada pelo receptor real, que possui uma chave de decodificação única e exclusiva (chave decifrante). A condição necessária para que o sistema seja seguro é que a chave decifrante seja mantida em sigilo.

De forma geral, são gerados dois pares de números – as chaves – onde a primeira chave (chave pública) apenas é decifrada quando utiliza-se a segunda chave (chave privada), porém, o primeiro número não pode ser derivado do primeiro.

---

[4]O código RSA leva as iniciais dos sobrenomes de seus criadores: Ronald L. Rivest, AdiShamir e Leonard M. Adleman, doutores do MIT (MassachussetsInstituteof Technology).

Dessa forma a chave pública pode ser publicada sem o risco de que a mensagem seja decifrada, a não ser que o outro agente possua a chave privada (STALLINGS, 2007).

A segurança do RSA vem do fato de que, por mais que seja fácil encontrar duas combinações grandes de números primos, como por exemplo combinações com mais de 100 números, é praticamente impossível factorizar o produto desses dois números (com um computador de alta capacidade, tal procedimento poderia levar milhares de anos para ser concluído).

Nos dias atuais, em diversos ramos de atividade os algoritmos RSA são utilizados, dentre os quais se destacam:

- Lojas Virtuais;
- Chips de Cartões de Crédito;
- Senhas de Bancos;
- Tokens;
- Certificados Digitais.

Através da exposição da história da criptografia, é clara a importância da inovação no seu desenvolvimento, saindo dos primórdios que escreviam com letras trocadas para dificultar a leitura por invasores, chegando aos dias atuais com algoritmos fatoriais que impossibilitam a invasão dos dados até mesmo pelos processadores mais potentes. Na próxima seção será analisada de forma conjunta a teoria apresentada com análise histórica da criptografia.

4 O DESENVOLVIMENTO DA CRIPTOGRAFIA SOB A ÓTICA DA TEORIA EVOLUCIONISTA

Analisando a história da criptografia, verificam-se avanços significativos na simplificação da utilização da mesma e na ampliação das suas áreas de uso, e isso só foi possível graças à inovação técnica. Nesta seção, analisar-se-á esse processo de inovação, com foco nos últimos oitenta anos (período de maiores mudanças e avanços dessa tecnologia), traçando paralelos com os fundamentos da Teoria Evolucionista que explicam quais foram às condições que proporcionaram um ambiente favorável para essa evolução.

Até 1932, o sistema de criptografia amplamente utilizado era o Código Morse, porém, devido ao baixo número de combinações que esse realizava, seu método apresentava falhas e sua capacidade de codificação não era grande o suficiente para garantir o sigilo das informações transmitidas. Através de estudos, e o envolvimento de matemáticosno processo de desenvolvimento do sistema, todos esses financiados pelo governo alemão através do serviço de inteligência do exército, chegou-se a um novo sistema muito mais robusto e de utilização simplificada: o Enigma G. O número de combinações desse novo sistema era muito superior ao do Código Morse, o que garantia maior confiabilidade ao sistema. Esse avanço só foi possível graças aos incentivos do governo alemão e pela utilização dos conhecimentos matemáticos aplicados.

A partir desse momento, observou-se que a utilização de métodos matemáticos era uma boa alternativa para o desenvolvimento de novas tecnologias para os sistemas de criptografia. Tanto foi dessa maneira, que os próximos sistemas criptográficos que surgiram tinham todos seus modelos básicos estruturados sobre algoritmos, fato esse que permiti centenas de milhares de combinações gerando ainda mais confiabilidade ao sistema.

E mais uma vez, a partir de uma demanda de um órgão de Estado, altos investimentos em pesquisas e desenvolvimento, e utilização do *know-how* adquirido através do desenvolvimento de sistemas anteriores, é desenvolvido um novo sistema de criptografia: o DES. Numa parceria público-privada, onde participaram pesquisadores da IBM, NIST e o NSA, foi desenvolvido esse sistema onde as mensagens eram enviadas, sem nenhuma necessidade de modificação na mensagem, porém, a mesma apenas poderia ser decifrada caso o receptor e o emissor possuíssem uma mesma senha para abrir a mensagem.

O sistema DES foi muito eficiente, tanto que foi utilizado pelo governo norte-americano até 2002, porém, pelo fato possuir uma única chave (o que implica na necessidade dos dois agentes transmissores da mensagem possuir uma mesma senha de forma prévia) e essa chave ser pequena, ou seja, vulnerável a ataques de computadores com boa capacidade de processamento, viu-se a necessidade de se desenvolver um novo sistema que corrigisse essas falhas, foi dessa demanda e dos constantes investimentos no desenvolvimento de novas tecnologias que surgiu o RSA.

O RSA tem o mesmo funcionamento do DES, porém, corrige as duas principais falhas que o sistema anterior. Através da implantação de uma chave assimétrica, ou seja, o sistema possui duas senhas diferentes que podem abrir a mesma informação, ele corrigiu o problema da necessidade dos agentes emissores e receptores necessariamente possuírem a mesma senha. E com o desenvolvimento de um novo modelo matemático, que utiliza a fatoração de números primos para codificação das mensagens, aumentou o nível de segurança do sistema, haja vista que até mesmo um computador com alta capacidade de processamento, poderia levar milhares de anos até encontrar a chave correta.

A chave RSA continua sendo amplamente utilizada, e em virtude das constantes demandas por novos setores da economia pelo sistema, o mesmo continua em processo de desenvolvimento, tanto para adaptação em novas rotinas, quanto na inovação em busca de novas soluções.

Ao observar o processo de inovação do sistema de criptografia a partir de sua história a fim de compreender de que forma a teoria evolucionista pode enxergar este fenômeno três aspectos devem ser mencionados quais sejam: a rotina, a aprendizagem e a trajetória tecnológica.

No que concerne à rotina das empresas ou no processo de inovação esta surge no ambiente evolucionista para revelar que o conhecimento somente é apreendido pelas firmas quando estas detêm certo grau de rotina e de aprendizagem. Nestes termos a rotina no sistema de criptografia surge nas empresas que detinham o conhecimento inserido nos seus sistemas de informação o que possibilitou o avanço e o seu aperfeiçoamento.

Quanto ao grau de aprendizagem, a firma evolucionista é entendida como um *locus* de acumulação de conhecimento, ou seja, somente a partir do conhecimento aprendido e transmitido é possível obtermos algum grau de inovação. O caso da criptografia a partir de sua história revela esta transmissão de um ponto da história aoutro onde o conhecimento é acumulativo e, portanto passívelde ser transferido. Apenas dessa maneira foi possível que o os EUA desenvolvessem a tecnologia RSA. A primeira maneira de aprendizado foi decifrando junto com o exército francês o Enigma G, que posteriormente sustentou o desenvolvimento do DES, que serviu de base para chegarem até ao sistema RSA.

Por fim, mas não esgotando o tema, a trajetória revela o inexorável avanço da ciência e, portanto da inovação nos ambientes de segurança. A trajetória

tecnológica dos sistemas de criptografia estão acompanhando os sistemas de segurança que impõem uma nova ordem globaldas informações, ou seja, um novo paradigma conforme assevera Giovani Dosi. Avaliando especificamente o caso da criptografia, em todos os momentos a necessidade por maior segurança na transmissão e armazenamento de informação se mostrou como sendo o paradigma que foi enfrentado, enquanto a trajetória encontrada em todos esses momentos foi a inovação.

Na próxima seção, será sumarizado todo material apresentado no trabalho, embasando as conclusões acerca do objeto de estudo.

5 CONCLUSÃO

A análise histórica do desenvolvimento dos sistemas de rede de informação, avaliando de forma específica o caso da criptografia e suas aplicações na indústria civil foi o objeto desse trabalho.

Na primeira seção analisamos os conceitos de Inovação, Ciência e Tecnologia sob a ótica da Teoria Evolucionista, e podemos destacar os pontos principais dessa Teoria:

1. O desenvolvimento tecnológico é um processo evolutivo, dinâmico, acumulativo e sistêmico;
2. A inovação não surge de maneira espontânea, mas sim de um processo de constante busca dos agentes;
3. Além de ser uma estratégia que parte de dentro das empresas, essa também é proveniente de uma resposta dessas as demandas do mercado;
4. Os fatores sociais e econômicos são determinantes no processo de desenvolvimento de novas tecnologias, principalmente no que diz respeito a atuação do Estado no incentivo a atividades consideradas por ele fundamentais;
5. O estágio de evolução tecnológico das empresas, o grau de incerteza, e os sinais de mercado, são fatores determinantes para o desenvolvimento ou não da inovação em determinados setores.

Na segunda seção do trabalho, foi realizada uma apresentação histórica da criptografia, iniciando sua análise a partir do Antigo Egito chegando até os dias atuais com a criptografia de redes.

Na terceira seção, analisou-se de forma paralela o processo histórico de desenvolvimento da criptografia, com os fundamentos teóricos da Teoria Evolucionista que dão embasamento para os fatores e condições que viabilizaram a evolução da criptografia.

Através da análise cruzada de todos os dados apresentados no trabalho, conclui-se que o processo de inovação tecnológico foi fundamental para o domínio da informação ocorrido com a criptografia, e esse pode ser explicado pela Teoria Evolucionista.

O processo de inovação da criptografia não foi algo que surgiu repentinamente, e foi um salto da criptografia escrita para com algoritmos, foi um processo lento e demorado que levou milênios até atingir o atual estágio de desenvolvimento.

Apesar de durante anos não apresentar inovações, muito em virtude da não necessidade de novas tecnologias, a criptografia teve um salto de qualidade a partir da II Guerra Mundial, muito em virtude da necessidade dos Estados em proteger suas informações, principalmente com o apoio dos Estados Unidos no desenvolvimento dos sistemas de criptografia de rede.

Sistema esse que quando desenvolvido serviu apenas para proteção de informações do Estado americano, hoje com o desenvolvimento da Internet e das novas formas de se relacionar da população, se tornou fundamental também na indústria civil, sendo alvo de altos investimentos por parte de empresas privadas visando aumentar a segurança de suas informações.

REFERÊNCIAS

BOUÇAS, C. FEBRABAN: Internet Banking vai superar transações de autoatendimento. **Valor Econômico**. Disponível em: <http://www.valor.com.br/empresas/2721580/febraban-internet-banking-vai-superar-transacoes-de-autoatendimento>. Acessoem: 13/03/2013

DOSI, G. **Technical Change and Economic Theory**. London: Pinter Publishers, 1988

DOSI, G. **Mudança Técnica e Transformação Industrial – A Teoria e Uma Aplicação à Indústria dos Semicondutores**. Campinas, Editora da UNICAMP, 2006.

FRANCO, W. B. A. **Criptografia**. Disponível em: <http://www.ucb.br/sites/100/103/TCC/22005/WaldizarBorgesdeAraujoFranco.pdf>. Acessoem: 08/03/2013

KAHN, D.**The Codebreakers, The Story of Secret Writing**. New York. The Macmillan Company, 1967

NELSON, R.R.; e WINTER S.G.**An Evolutionary Theory of Economic Change.** Harvard University Press Cambridge, 1982

SCHUMPETER, J.**The Theory of Economic Development**.Harvard University Press Cambridge, 1934

SINGH, S. **O Livro dos Códigos**, Editora Record, São Paulo, 2004

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e Pratica**, São Paulo, Pearson, 2007